

The copyright of this thesis vests in the author. No quotation from it or information derived from it is to be published without full acknowledgement of the source. The thesis is to be used for private study or non-commercial research purposes only.

Published by the University of Cape Town (UCT) in terms of the non-exclusive license granted to UCT by the author.

Design and Implementation of a Digital Real-Time Secondary Surveillance Radar/Identification Friend or Foe Target Emulator

Sharef Neemat

Thesis presented for the degree of Masters of Science in Engineering
In the Department of Electrical Engineering
University of Cape Town

July 2010

DECLARATION

I know the meaning of plagiarism and declare that all the work in the document, save for that which is properly acknowledged, is my own.

Signature of Author

9 July 2010

University of Cape Town

ABSTRACT

SSR/IFF interrogator signal processors are typically required to identify replies from up to 1500 target transponders per antenna rotation.

A real live test involving such a large number of targets would be extremely expensive, and difficult to repeat. There is thus a need for specialized target emulators to be developed and used as laboratory test equipment.

This thesis describes the design and implementation of a transistor-transistor-logic (TTL) real-time SSR/IFF target emulator. User requirements that describe the system are captured and analyzed, resulting in the generation of a system breakdown structure; a summary of the relevant concepts and requirements allocation process for each subsystem is presented, in order to produce a technical specification for the system.

The developed target emulator runs on the Innovative Integration Quixote board, and is capable of generating SSR/IFF replies for modes 1, 2, 3/A, C and secure mode 4 from up to 4000 emulated mobile targets at ranges from 0 to 600km. On the Quixote, a Xilinx VirtexII FPGA implements real-time aspects of the design, while target configuration information is continuously maintained by a Texas Instruments TMS320C6416 DSP for each antenna rotation. Emulated target configuration parameters are fully reconfigurable on-the-fly in terms of range, azimuth and reply codes in order to allow the user to create numerous test scenarios.

The operation of the target emulator has been verified against all design requirements, and it has been found to be compliant. The verification was performed using co-simulation and on-target testing methods. The Quixote board is a suitable HW platform for the system; however, it has been recommended that a lower cost board should be used in the future.

To My Family

University of Cape Town

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to the Almighty Allah for providing me with the necessary strength to conclude this study.

I am especially thankful to my supervisor, Professor M.R. Inggs for allowing me the opportunity to complete my MSc at the RRSg, and for his guidance and time. I would also like to thank Hatim Behairy for his support and patience throughout the duration of this Masters project.

This work would not have been completed without the design ideas and advice from Peter Koeppen, and for that, I am grateful. I am particularly thankful to Clive Bowerman for helping me to settle in Cape Town and for sharing his advice on everything from Braai secrets to advanced electronics!

Many thanks go to Keith Dowson for answering all my SSR/IFF questions.

I would also like to thank Saleh Alsaif and Suliman Alalit for their comradeship and morale!

I must also thank Regine Lord for the valuable advice and Bianca Tosolari for her friendship and for challenging every line of this thesis.

Lastly, I would like to thank Norah Jones for the great company!

CONTENTS

DECLARATION.....	II
ABSTRACT.....	III
ACKNOWLEDGEMENTS	V
1. CHAPTER 1: INTRODUCTION	2
1.1 SSR/IFF BACKGROUND.....	3
1.2 PRIMARY VS SECONDARY RADAR	4
1.3 SSR/IFF MAJOR SYSTEM COMPONENTS AND TOP LEVEL PROJECT SCOPE	5
1.4 THESIS OUTLINE	7
1.4.1 Chapter 2: User Requirements	8
1.4.2 Chapter 3: System Concepts and Requirements Allocation.....	8
1.4.3 Chapter 4: System Design.....	9
1.4.4 Chapter 5: System Implementation	9
1.4.5 Chapter 6: System Testing and Results	9
1.4.6 Chapter 7: Conclusions and Future Work	10
1.5 SUMMARY	10
2. CHAPTER 2: USER REQUIREMENTS	11
2.1 FUNCTIONAL REQUIREMENTS.....	11
2.1.1 TxP and TCC Emulation.....	11
2.1.2 SSR/IFF Reply Modes.....	11
2.1.3 Number of Targets	11
2.1.4 Distinct Target Identity.....	12
2.1.5 Friendly and Non-Friendly Targets.....	12
2.1.6 Real-time Operation.....	12
2.1.7 Continuous Operation	12
2.1.8 Target Mobility and Space.....	12
2.1.9 Garbled and FRUIT Replies	12
2.1.10 Antenna Interface	13

2.2	HW REQUIREMENTS	13
2.3	REQUIREMENTS FOR FUTURE USE	14
2.4	SUMMARY	14
3.	CHAPTER 3: SYSTEM CONCEPTS AND REQUIREMENTS ALLOCATION.....	15
3.1	USER REQUIREMENTS ANALYSIS	15
3.2	SUBSYSTEM CONCEPT SUMMARIES INTRODUCTION	17
3.3	REQUIREMENTS ALLOCATION INTRODUCTION	18
3.4	TXP CONCEPT SUMMARY AND REQUIREMENTS	18
3.4.1	SSR/IFF TxP Concept Summary	18
3.4.2	SSR/IFF TxP Requirements.....	27
3.5	TCC CONCEPT SUMMARY AND REQUIREMENTS.....	38
3.5.1	IFF TCC Concept Summary.....	38
3.5.2	IFF TCC Requirements	39
3.6	FRUIT AND GARBLED REPLIES CONCEPT SUMMARIES AND REQUIREMENTS	41
3.6.1	FRUIT Replies Concept Summary.....	41
3.6.2	Garbled Replies Concept Summary	43
3.6.3	FRUIT and Garble Requirements	46
3.7	INTERROGATOR CONCEPT SUMMARY AND REQUIREMENTS	46
3.7.1	SSR/IFF Interrogator Concept Summary	46
3.7.2	SSR/IFF Interrogator Requirements.....	47
3.8	ICC CONCEPT SUMMARY AND REQUIREMENTS	48
3.8.1	IFF ICC Concept Summary	48
3.8.2	IFF ICC Requirements	49
3.9	TARGET IDENTITY GENERATOR CONCEPT SUMMARY AND REQUIREMENTS.....	51
3.9.1	Target Identity Generator Requirements.....	51
3.10	TARGET MOBILITY MANAGER CONCEPT SUMMARY AND REQUIREMENTS	52
3.10.1	Target Mobility Manager Concept Summary	52
3.10.2	Target Mobility Manager Requirements.....	58
3.11	CONTINUOUS OPERATION MANAGER CONCEPT SUMMARY AND REQUIREMENTS.....	59
3.11.1	Continuous Operation Manager Requirements	59
3.12	REAL-TIME OPERATION MANAGER CONCEPT SUMMARY AND REQUIREMENTS.....	60

3.13	ITRC INTERFACE REQUIREMENTS.....	60
3.14	HW INTERFACE REQUIREMENTS.....	60
3.15	USER REQUIREMENTS TRACEABILITY MATRIX.....	61
3.16	SUMMARY	61
4.	CHAPTER 4: SYSTEM DESIGN.....	63
4.1	TARGET HW OVERVIEW.....	63
4.2	SSR/IFF EMULATOR TOP-LEVEL BLOCK DIAGRAM.....	64
4.3	SSR/IFF EMULATOR CONCEPT DESIGN SUMMARY	64
4.4	DESIGN PARTITIONING DECISIONS.....	66
4.4.1	FPGA Partition.....	66
4.4.2	DSP Partition	66
4.5	SSR/IFF TARGET EMULATOR FPGA DETAILED DESIGN.....	67
4.5.1	TxP and TCC Design	72
4.6	SSR/IFF TARGET EMULATOR DSP DETAILED DESIGN	77
4.6.1	DSP-FPGA Asynchronous Memory Interface.....	77
4.6.2	Lookup Table and Targets Configuration information.....	79
4.6.3	DSP SW Design	81
4.7	ADDITIONAL SYSTEM DESIGN CONSIDERATIONS AND NOTES.....	83
4.8	SUMMARY	84
5.	CHAPTER 5: SYSTEM IMPLEMENTATION.....	85
5.1	FPGA DESIGN IMPLEMENTATION	85
5.1.1	FPGA Implementation Tool-Chain	85
5.1.2	Matlab/Simulink FPGA Implementation, Co-Simulation and Rapid Prototyping.....	86
5.1.3	VHDL Code Portability	88
5.2	DSP SW IMPLEMENTATION	88
5.2.1	SW Implementation Methodology	88
5.2.2	SW Portability	89
5.2.3	DSP Interrupt Vector Table and Memory Command File Creation	89
5.3	FPGA AND DSP SOURCE CODE.....	89
5.4	FPGA AND DSP RESOURCE UTILIZATION.....	90

5.5	ADDITIONAL IMPLEMENTATION CONSIDERATIONS.....	91
5.6	SYSTEM LIMITATIONS.....	91
5.7	SUMMARY	92
6.	CHAPTER 6: SYSTEM TESTING AND RESULTS.....	93
6.1	SYSTEM DEMONSTRATION AND TESTING METHODOLOGY	93
6.2	CO-SIMULATION TESTS.....	96
6.2.1	SIF Mode Intervals	97
6.2.2	SIF Mode Intervals Tolerance	97
6.2.3	SIF Mode Interrogation Pulse Width Validation.....	99
6.2.4	SIF Mode SPI/Emergency Replies	99
6.2.5	Mode 4 Processing.....	101
6.2.6	TxP-TCC SIF/Mode 4 Internal Suppression and Performance	102
6.3	REAL-TIME ON-TARGET TESTS	103
6.3.1	Target Creation and Programmability Tests.....	104
6.3.2	FRUIT Interrogators Test	108
6.3.3	Garbled Replies Test	109
6.3.4	Maximum number of targets test.....	116
6.4	SUMMARY	116
7.	CHAPTER 7: CONCLUSIONS AND FUTURE WORK	118
7.1	PROJECT SUMMARY AND CONCLUSIONS	118
7.2	RECOMMENDATIONS AND FUTURE WORK.....	118
	APPENDIX A : USER REQUIREMENTS TRACEABILITY MATRIX	123
	APPENDIX B : SOURCE CODE.....	126
B.1	FPGA VHDL CODE	126
B.2	DSP C CODE	127
B.3	MATLAB/SIMULINK MODELS	127
B.4	HIGH RESOLUTION SYSTEM TEST RESULTS IMAGES	128

LIST OF FIGURES

Figure 1.1 : Typical SSR/IFF system components.....	6
Figure 1.2 : Thesis overview.....	7
Figure 2.1 : Innovative Integration Quixote [8] board.....	13
Figure 3.1 : SSR/IFF target emulator system breakdown structure.....	17
Figure 3.2 : From [1]. SSR interrogation signal format.....	19
Figure 3.3 : General reply format of SSR SIF modes (adapted from [2]).....	20
Figure 3.4 : From [2]. SSR Timing Diagram for Modes 1, 2, 3/A and C.....	22
Figure 3.5 : Adopted from [2]. IFF Secure Mode 4.....	23
Figure 3.6 : Example of secure mode 4 reply validation algorithm.....	24
Figure 3.7 : Secure mode 4 All pulse scenario.....	25
Figure 3.8 : From [2]. IFF timing diagrams for secure mode.....	26
Figure 3.9 : From [3]. SSR/IFF Interrogator Antenna Patterns.....	27
Figure 3.10 : IFF secure mode 4 interrogation decryption sequence.....	39
Figure 3.11 : Example of a FRUIT situation in SSR/IFF.....	43
Figure 3.12 : Examples of garbling.....	45
Figure 3.13 : IFF secure mode 4 interrogator to ICC interaction.....	49
Figure 3.14 : The ACP pulse count represents the azimuth.....	53
Figure 3.15 : ACP spacing is the time between two ACP pulses.....	54
Figure 3.16 : The emulated target labelled "X" is assumed to be.....	56
Figure 3.17 : Recalling Figure 3.16, the emulated target labelled "X".....	58
Figure 4.1 : From [14]. The two main computers on the Quixote.....	63
Figure 4.2 : SSR/IFF target emulator top-level block diagram.....	64
Figure 4.3 : Eight TxP-TCC pairs are divided into two groups, A and B.....	69
Figure 4.4 : SSR/IFF target emulator FPGA design.....	71
Figure 4.5 : TxP-TCC block diagram showing the inputs and outputs.....	73

Figure 4.6 : TxP and TCC CC interrogation detection and reply process.....	75
Figure 4.7 : Target information look-up tables ping-pong usage illustration...	79
Figure 4.8 : Detailed design of the TI TMS320C6416 DSP code.....	82
Figure 5.1 : From [9]. Simulink VHDL co-simulation, HW in-the-loop.....	86
Figure 5.2 : Simulink implementation of a pulse width discriminator.....	87
Figure 5.3 : Simulink blocks are replaced with VHDL blocks.....	88
Figure 5.4 : FPGA resource utilization summary produced by Xilinx.....	90
Figure 5.5 : DSP internal and external memory utilization summary.....	91
Figure 6.1 : SSR/IFF target emulator test setup.....	94
Figure 6.2 : Co-simulation TxP-TCC and FRUIT interrogator test.....	95
Figure 6.3 : Example of co-simulation testing parameters.....	96
Figure 6.4 : TxP-TCC pair does not reply to an undefined SIF.....	97
Figure 6.5 : TxP-TCC pair replies to a mode 2 interrogation.....	98
Figure 6.6 : A reply group pulse width is 0.450 μ s as expected for a SIF.....	98
Figure 6.7 : TxP-TCC pair does not reply to a mode 2 interrogation.....	99
Figure 6.8 : TxP-TCC pair generating an SPI reply that comprises two.....	100
Figure 6.9 : TxP-TCC pair generating an emergency reply that comprise...	100
Figure 6.10 : TxP-TCC replying in the last reply position.....	101
Figure 6.11 : TxP-TCC does not reply to a challenge missing the first All...	102
Figure 6.12 : Three mode 1 interrogations injected to the TxP-TCC.....	103
Figure 6.13 : Three mode 4 interrogations injected to the TxP-TCC.....	103
Figure 6.14 : The code snippet presented is used to create two test.....	104
Figure 6.15 : The mode enabled target between ACPs 2000 and 2020.....	106
Figure 6.16 : The first target is between ACPs 10 and 60.....	107
Figure 6.17 : Interrogations from two different interrogators are shown.....	108
Figure 6.18 : FRUIT reply scenario. During ACP 17, the first reply is.....	109

Figure 6.19 : Targets crossing scenario. When the targets are at.....	110
Figure 6.20 : Code snippet used to create test targets for the garbled.....	111
Figure 6.21 : Replies from two targets with different reply codes.....	112
Figure 6.22 : Continued sequence of garbling test result from	113
Figure 6.23 : Continued sequence of garbling test result from.....	114
Figure 6.24 : Continued sequence of garbling test result from.....	115
Figure 6.25 : A magnified view of the garbling scenario.....	116
Figure 7.1 : FPGA subdirectory. VHDL files for the FPGA.....	126
Figure 7.2 : DSP subdirectory. C source code, interrupt vector file.....	127
Figure 7.3 : Simulink subdirectory. Simulink co-simulation and TxP.....	127
Figure 7.4 : System test results images subdirectory	128

LIST OF TABLES

Table 3.1 : From [1]. Common SSR Interrogation Modes Summary.....	20
Table 3.2 : From [1]. SSR Data Pulses Designation.....	21
Table 3.3 : SSR P1 to P3 Pulse intervals and Tolerances.....	28
Table 3.4 : SSR Interrogation Pulses Duration and Tolerances.....	28
Table 3.5 : IFF Secure Mode 4 Pulse Intervals and Tolerances.....	29
Table 3.6 : IFF Secure Mode 4 Pulse Durations.....	30
Table 3.7 : Mode 4 Enable Trigger Timing and Tolerances.....	31
Table 3.8 : Non-Secure Modes Reply Timing Characteristics.....	32
Table 3.9 : From [2]. Non-Secure Modes Reply Pulse Positions from F1.....	33
Table 3.10 : From [2]. Modes 1, 2, 3/A and C Reply Code Designation.....	34
Table 3.11 : From [2]. Modes 1, 2, 3/A and C Employed Reply Pulses.....	34
Table 3.12 : From [2]. Emergency Reply Groups Timing from First Reply.....	35
Table 3.13 : IFF Secure Mode 4 Reply Timing Characteristics.....	36
Table 3.14 : SSR/IFF emulator input/output signals.....	61
Table 4.4.1: Antenna ACP Count (ACPC) register bits allocation.....	67
Table 4.2: Interrupt Pending Register (IPR) bits allocation.....	68
Table 4.3: Interrogator(x) Information Register (IIRx) bits allocation.....	70
Table 4.4: Plain Text M4 Challenge Definition.....	74
Table 4.5: TxP(x) Information Register (TIR) Bits Allocation. (1 = enable)....	76
Table 4.6: TxP(x) Delay Register (TDR) Bits Allocation.....	76
Table 4.7: TCC(x) Key Register (TKR) Bits Allocation.....	76
Table 4.8 : FPGA registers and their addresses.....	77
Table 4.9 : Target configuration look-up table format.....	80
Table 4.10 : Target information structure format	81

Table 7.1 : User Requirements Traceability Matrix.....	122
--	-----

University of Cape Town

NOMENCLATURE

ACP	Azimuth Change Pulse
ADC	Analogue-to-Digital Converter
ARP	Azimuth Reference Pulse
All	Anti Interference Interrogation
ATC	Air Traffic Control
CC	Cryptographic Computer
CCS	Code Composer Studio
cPCI	Compact Peripheral Component Interconnect
DAC	Digital-to-Analogue Converter
DOD	Department of Defence
DSP	Digital Signal Processing/Processor
EBW	Effective Beam Width
EMIF	External Memory Interface
FIFO	First In First Out
FPGA	Field Programmable Gate Array
FRUIT	Friendly Reply Unsynchronized in Time
GUI	Graphical User Interface
HW	Hardware
ICC	Interrogator Cryptographic Computer
IDE	Integrated Development Environment
IFF	Identification Friend or Foe
IIRx	Interrogator(x) Information Register (IIRx)
INT	Interrogator
IPR	Interrupt Pending Register
ISLS	Interrogator Side-Lobe Suppression
ISR	Interrupt Service Routine

NOMENCLATURE

ITRC	IFF Transceiver Card
JTAG	Joint Test Action Group
LUT	Lookup Table
MISRA	Motor Industry Software Reliability Association
ns	Nanoseconds
NATO	North Atlantic Treaty Organization
OS	Operating System
PCI	Peripheral Component Interconnect
PPI	Plan Position Indicator
PRF	Pulse Repetition Frequency
PRI	Pulse Repetition Interval
PT	Pre-Trigger
QTR	Qualification Test Results
RF	Radio Frequency
RRSG	Radar Remote Sensing Group
RV	Reply Video
SBSRAM	Synchronous Burst Static Random Access Memory
SDRAM	Synchronous dynamic random access memory
SIF	Selective Identification Feature
SLS	Side Lobe Suppression
SM	Secure Mode
SPI	Special Position Indicator
SSR	Secondary Surveillance Radar
STANAG	Standardization Agreement
SUM	Sum channel of the antenna

NOMENCLATURE

TCC	Transponder Cryptographic Computer
TDR	TxP(x) Delay Register
TDV	Time Decoded Video
TIR	TxP(x) Information Register
TKR	TCC(x) Key Register
TTL	Transistor-Transistor Logic
TxP	Transponder
TxP-TCC	Transponder-TCC Pair
UCF	User Constraints File
UCT	University of Cape Town
VHDL	VHSIC Hardware Description Language
VHSIC	Very-High-Speed Integrated Circuit
μ s	Micro Seconds
XOR	Exclusive or

1. Chapter 1: Introduction

The aim of this thesis is to describe the design, implementation and testing of a digital, real-time Secondary Surveillance Radar/Identification Friend or Foe (SSR/IFF) target emulator. This emulator has been designed to test and debug an SSR/IFF interrogator digital signal processor, and is intended for use in a laboratory setting. The design of the target emulator also provides a foundation for the future development of SSR/IFF equipment.

Once the target emulator has been set up and interrogated by an interrogator, it is capable of generating STANAG-4193 [2] digital TTL timing compliant SSR/IFF replies simultaneously from thousands of simulated mobile targets. These targets are equipped with SSR/IFF transponders and cryptographic computers, each with distinct, user defined reply codes for modes 1, 2, 3/A, C and secure mode 4. The emulator will also have the ability to generate SSR emergency and Special Position Indicator (SPI) responses.

The target emulator is able to interface with a SSR/IFF antenna or to emulate the azimuth pulse behaviour of an idle SSR/IFF antenna, if an antenna is not present. Emulated targets can be scattered within a 360° panoramic view, all in correspondence to the antenna azimuth pulses.

The target emulator is designed to test the ability of an interrogator signal processor to identify the emulated targets correctly, as well as to de-garble overlapped replies and to de-correlate Friendly Replies Unsynchronized in Time (FRUIT) properly. It is also designed to test whether the interrogator will correctly decode and assign replies to targets on the interrogator display. The target emulator carries out these tests while creating a continuous live testing environment for the user, in the sense that the user is given the option to alter interrogation parameters on-the-fly, i.e. target locations and ranges, target mobility behaviour, and FRUIT interrogators' interrogation modes, without the need to stop or pause the emulator.

A significant portion of the design and implementation was done using VHDL co-simulation techniques, which makes allowance for mixing and integration of Matlab/Simulink [11] blocks with C code running in the Matlab/Simulink

environment, and with VHDL code running in Modelsim [10], which are all controlled by Matlab/Simulink.

1.1 SSR/IFF Background

In primary radar, a reasonably high powered pulse is transmitted through space towards a target. The radar then detects the presence of that target when a part of the energy is reflected back from the target's surface. The radar is also able to calculate the target's range by measuring the time from the transmission of the pulse to the time the reflection is received [1]. In Secondary Surveillance Radar (SSR) the purpose is neither to detect the presence of the target nor to determine its position accurately, but rather to identify the target positively and to distinguish it from other targets.

In order for a target to be identified, it must be equipped with a special transceiver known as an SSR transponder, which receives coded pulses of energy at a frequency of 1030 MHz. Together, these pulses form what are known as "interrogations" or "challenges", which are generated by an SSR interrogator. After processing an interrogation, the transponder replies by transmitting coded pulses containing identification information at a frequency of 1090 MHz. The interrogator receives a reply and interprets it, before passing the result to a display system in the simplest application, or to a larger command and control system.

SSR is currently being used in the military and in civilian Air Traffic Control (ATC) systems. In the military, the need to identify friendly aircrafts positively first arose during the Second World War. Military use of SSR is known as Identification Friend or Foe (IFF) [1]. The information from the IFF system forms part of the decision aid process, which must be followed before a weapon is fired, or action is taken against a non-friendly target.

During military training or conflict, a secure IFF mode is used to identify friendly targets, using Cryptographic Computers (CCs) connected to the interrogator and the transponder. The interrogator CC typically generates encrypted interrogation pulses and informs the interrogator *when* to expect a reply if a friendly platform has successfully decrypted the interrogation. When the transponder receives an encrypted interrogation, it passes it to the

attached CC, and if the CC successfully decrypts the interrogation, it informs the transponder when to generate the reply. The interrogator identifies a target as a friend only if it correctly replies to a specific number of secure interrogations in the correct time windows.

In 1996, the USA Department of Defence (DOD) Command Joint Chief of Staff directed that “all DOD Aircraft IFF systems be fully operational in order to render aircraft mission capable” [7].

The technical characteristics of SSR/IFF are governed by the Standardization Agreement, known as the STANAG-4193 document, which was created by the North Atlantic Treaty Organization (NATO) [2] military agency for standardization.

1.2 Primary vs Secondary Radar

Primary and secondary radar are often used jointly, and in most cases their antennas rotate simultaneously [3]. The primary radar typically detects a target, whereas the secondary radar determines the target's reported identity and altitude, in order to identify it as a friend or a foe.

In congested aircraft traffic, a traditional ATC Plan Position Indicator (PPI), and even a more modern display system would tend to become cluttered, especially if information is only displayed from the primary radar. In such cases, it can become extremely difficult to relate a blip on the screen to a target in the sky, even if their flight plans are known to the ATC operator. The secondary radar provides additional information from the aircraft transponder, which, if used in conjunction with the information provided by the primary radar, facilitates easier manual or automatic tracking of targets on the ATC display.

The power needed to transmit an interrogation in SSR is significantly less than what is needed for primary radar operating at the same range, due to the two-way nature of the link in SSR. The transmitter need only generate enough power for the interrogation to be detected by the transponder. There is no need to cater for losses resulting from the return path, as in the case of primary radar, which results in longer cover at a lower power cost. Unwanted echoes are not picked up and clutter is avoided in SSR, because the

transmitter and the receiver are not in tune with each other, as they use different frequencies to transmit and receive interrogations/replies as described in Section 1.1 and reference [3]. SSR thus costs a fraction of the cost of an equivalent primary radar [1].

1.3 SSR/IFF Major System Components and Top Level Project Scope

The main components of SSR/IFF systems as depicted in Figure 1.1 are:

- **Antennas:** Interrogator systems are typically equipped with directional antennas. Transponders usually receive and transmit their replies via one or two omnidirectional antennas.
- **Transponders:** These are transceivers with the capability of receiving electronic challenges from interrogators in order to process them and to transmit an appropriate reply [4]. Transponders can be ground-based, ship-based or airborne.
- **Interrogators:** These are transceivers with the capability of transmitting electronic challenges and receiving replies from target transponders. These replies are processed in order to determine the targets' identity, position and range. Interrogators can similarly be ground-based, ship-based or airborne.
- **Cryptographic Computers:** These provide for a secure encrypted challenge/reply operation, and they are used in conjunction with interrogators and transponders.
- **Displays:** Interrogator systems are typically connected to PPIs or more modern display systems, where the positions and identities of targets are graphically presented. These displays can be shared with or separate from the primary radar display.

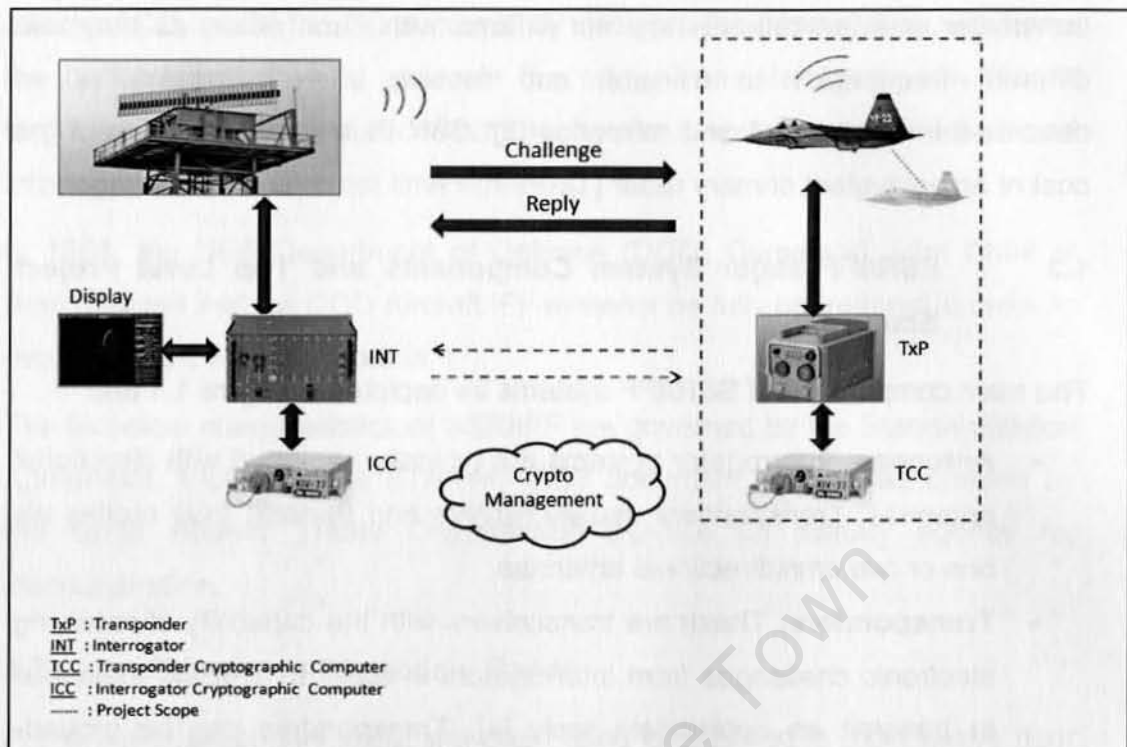


Figure 1.1 : Typical SSR/IFF system components. The box created by the dashed lines and arrows represents the top level project scope, which is to emulate the TTL timing behaviour of hundreds of distinct identity SSR/IFF transponders and their CCs, which are fitted onto mobile targets. When interrogated, the system will provide STANAG-4193 [2] timing compliant replies, including garbled and FRUIT reply scenarios simultaneously from the emulated targets, *bypassing the RF link* and feeding directly into the interrogator signal processor. In order to cater for effects caused by having multiple interrogators in close range to the interrogator being tested, some basic aspects of SSR/IFF interrogators and interrogator cryptographic computers (ICCs) are also emulated.

1.4 Thesis Outline

The structure of this thesis is illustrated in Figure 1.2 below.

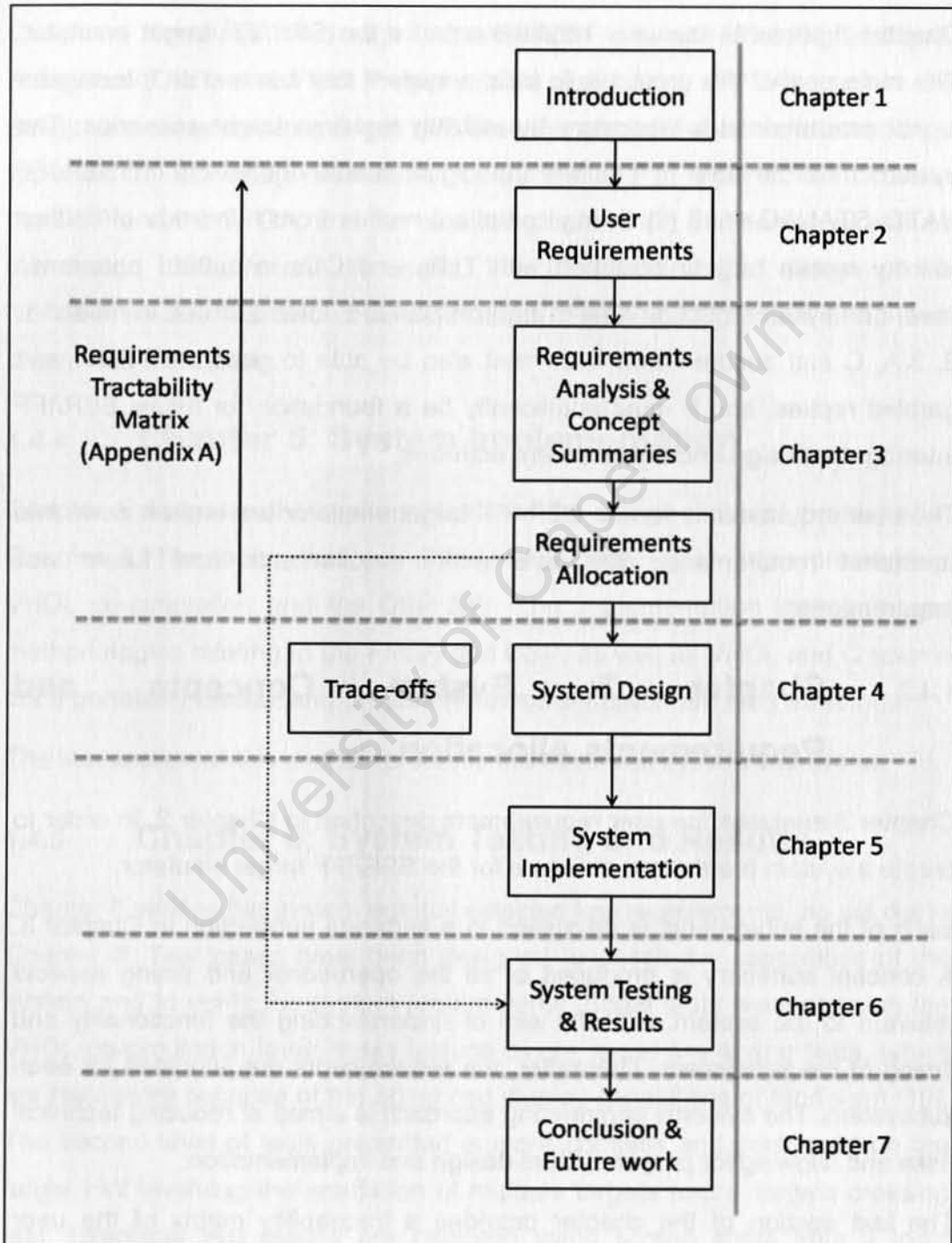


Figure 1.2 : Thesis overview

The following subsections provide short summaries of each of the forthcoming chapters in the thesis.

1.4.1 Chapter 2: User Requirements

Chapter 2 captures the user requirements for the SSR/IFF target emulator. The main goal of this project is to build a system that can test an interrogator signal processor in a laboratory by utilizing real-time target scenarios. The system must be able to emulate the digital domain behaviour of SSR/IFF NATO STANAG-4193 [2] timing compliant replies from hundreds of distinct identity mobile targets equipped with TxPs and CCs in a 360° panoramic view. The system must be able to support SSR/IFF interrogations in modes 1, 2, 3/A, C and secure mode 4. It must also be able to generate FRUIT and garbled replies, and it must additionally be a foundation for future SSR/IFF interrogator design and development activities.

The user requirements for the SSR/IFF target emulator are broken down into functional requirements, hardware (HW) requirements and future use requirements.

1.4.2 Chapter 3: System Concepts and Requirements Allocation

Chapter 3 analyses the user requirements described in Chapter 2, in order to create a system breakdown structure for the SSR/IFF target emulator.

Each of the subsystems is discussed in a separate subsection in Chapter 3. A concept summary is produced of all the operational and timing aspects relevant to the system, with the aim of understanding the functionality and timing of the subsystem. Thereafter, the requirements are allocated for each subsystem. The systems engineering approach is aimed at reducing technical risks and allowing for proper system design and implementation.

The last section of the chapter provides a traceability matrix of the user requirements (Table 7.1), which maps the user requirements as set out in Chapter 2, and the relevant derived requirements as described in Chapter 3.

This traceability matrix guarantees that all user requirements have been considered in the design and implementation of the system.

1.4.3 Chapter 4: System Design

Chapter 4 discusses the design of the SSR/IFF emulator. The Digital Signal Processor (DSP) and Field Programmable Gate Array (FPGA) used in the design are presented in a target HW overview section, which is followed by a top-level concept design summary. The system design is partitioned between the DSP and the FPGA, and the reasoning behind the partitioning as well as the design tradeoffs are discussed. The low-level detailed design of the SSR/IFF emulator is also covered in depth. Figure 4.2 illustrates a top-level diagram of the system.

1.4.4 Chapter 5: System Implementation

Chapter 5 discusses the implementation of the design that was presented in Chapter 4. The topics that are discussed include FPGA rapid prototyping, VHDL co-simulation and the DSP SW. The implementation tool-chain and methodologies relating to the FPGA and DSP, as well as VHDL and C source code portability issues, and devices resource utilization are also examined.

The last section of this chapter presents the observed system limitations.

1.4.5 Chapter 6: System Testing and Results

Chapter 6 verifies the system against selected key requirements, as set out in Chapter 3. Test cases have been designed to check the capabilities of the system and to verify the system requirements. Some tests were done on the VHDL co-simulation level; these include single target fine timing tests, which are necessary because of the advanced display capabilities of Modelsim [10]. The second level of tests presented is more complex and performed on the target HW involving the emulation of multiple targets and a targets crossing test. Graphical test results are captured using screen shots from a logic analyser and are presented after each test.

1.4.6 Chapter 7: Conclusions and Future Work

Chapter 7 summarises and concludes the SSR/IFF target emulator project. The system is found to be compliant with requirements, except for the system limitations discussed in Chapter 5. Recommendations to port the design to a cheaper board and possible areas of future improvement are discussed.

1.5 Summary

This chapter has introduced the SSR/IFF emulator project, which is the purpose of this research. It has also provided the background to SSR/IFF, briefly comparing this with primary radar, and a summary of the major system components of the SSR/IFF system from a top-level perspective. A brief thesis overview describing each of the succeeding chapters has also been presented. The following chapter aims to capture the user requirements for the SSR/IFF emulator system, which are divided into functional requirements, HW requirements and future use requirements.

2. Chapter 2: User Requirements

The SSR/IFF target emulator is required to be a real-time laboratory system, which is used to test and debug an SSR/IFF interrogator signal processor. When the system is interrogated, it is required to generate STANAG-4193 [2] digital timing compliant replies from mobile targets that are equipped with SSR/IFF TxPs and CCs. Each of these targets have distinct user-defined SSR/IFF modes 1, 2, 3/A (identification response), C (aircraft altitude response) and secure mode 4 reply codes, which exist in a 360° panoramic view. The system is additionally required to generate other effects, to which the interrogator may be exposed, such as FRUIT.

The functional requirements for the SSR/IFF target emulator are listed in Section 2.1, whereas HW and future use requirements are listed in Sections 2.2 and 2.3.

2.1 Functional Requirements

The SSR/IFF target emulator must be capable of performing the following functions:

2.1.1 TxP and TCC Emulation

The system must be able to emulate the digital timing behaviour of STANAG-4193 [2] compliant SSR/IFF TxPs and Transponder Cryptographic Computers (TCCs) when validating received interrogations and generating replies thereto.

2.1.2 SSR/IFF Reply Modes

When it is enabled to do so, the system must be able to generate STANAG-4193 [2] SSR/IFF replies in modes 1, 2, 3/A, C and secure mode 4, as well as emergency and SPI replies.

2.1.3 Number of Targets

In a single antenna sweep, the system must be able to produce SSR/IFF replies from 0 to 1,500 emulated targets equipped with SSR/IFF TxPs and CCs. The targets may be evenly distributed in 360°.

2.1.4 Distinct Target Identity

Each emulated target must utilise distinct, user definable, and SSR/IFF STANAG-4193 [2] compliant reply codes for modes 1, 2, 3/A, C.

2.1.5 Friendly and Non-Friendly Targets

The system must be able to emulate both friendly and non-friendly secure mode 4 targets.

2.1.6 Real-time Operation

The system must operate in a real-time mode, which means that the amount of time it takes from the instant in which the system receives an interrogation to the time it generates the emulated replies must be proportional to both the ranges of the emulated targets, and the STANAG-4193 [2] requirements, for the maximum time allowed for a TxP and a TCC to process received interrogations and generate replies thereto.

2.1.7 Continuous Operation

The system must operate in a continuous live mode, which means that it must react to interrogation parameter changes received on-the-fly (i.e. Pulse Repetition Frequency (PRF), interrogation modes, target location and range, etc.) set by the user, without the user needing to stop or pause the system in order to change the settings.

2.1.8 Target Mobility and Space

The system must be able to emulate mobile targets equipped with SSR/IFF TxPs and TCCs moving within 360° and at a range of from 0 to 600km and a mode C altitude from -1,000 feet to 121,000 feet.

2.1.9 Garbled and FRUIT Replies

The system must be able to create both garbled and FRUIT SSR/IFF reply scenarios in modes 1, 2, 3/A, C and secure mode 4.

2.1.10 Antenna Interface

The system must be able to receive Azimuth Change Pulses (ACP) and Azimuth Reference Pulses (ARP) from an IFF antenna, which completes a full rotation in 8 seconds and provides 4096 ACP counts per rotation. If the antenna is not available at any given time, the system must also be able to generate the ACP/ARP pulses and supply them to the interrogator being tested. The antenna Effective Beam Width (EBW) is 5°.

2.2 HW Requirements

The emulator must be designed and implemented to run on the Innovative Integration Quixote [8] DSP board shown in Figure 2.1. Information about the board is available on the official Innovative Integration [8] website. A suitable off-the-shelf cPCI solution, which contains a single board computer running Windows XP, and a card-cage with a cPCI backplane, has been chosen for the Quixote to plug into it. If communication via the cPCI bus is deemed unnecessary, Joint Test Action Group (JTAG) may be used as an alternative in order to communicate with the DSP and the FPGA.

The input/output of the emulator must be made available from/to the interrogator signal processor via the digital input/output general purpose pins, which are available on the board.

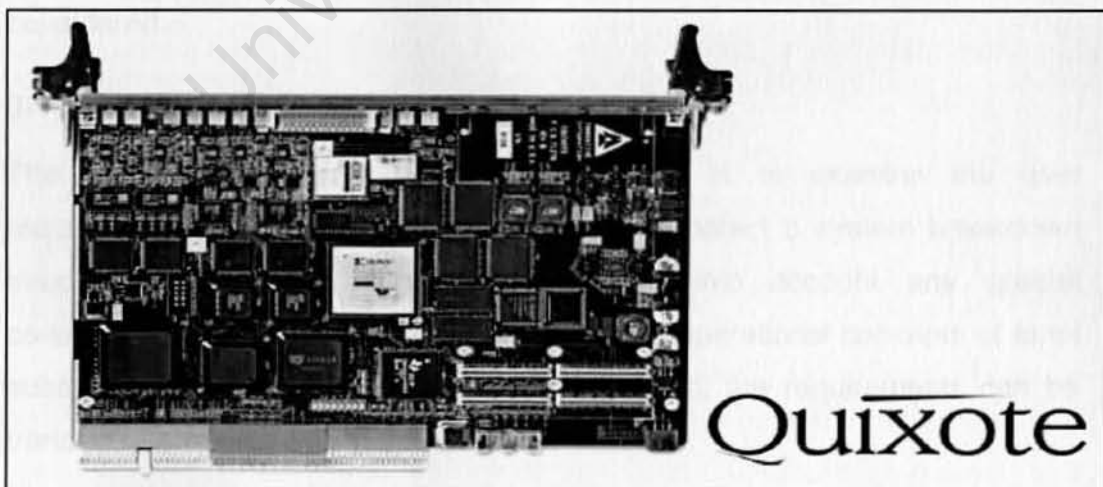


Figure 2.1 : Innovative Integration Quixote [8] board

2.3 Requirements for Future Use

The IFF Transceiver Card (ITRC) is an RF SSR/IFF test transceiver card that is currently being developed by another Masters student in the Radar Remote Sensing Group (RRSG) at the University of Cape Town. The system presented in this thesis must suggest an interface point in order to allow the ITRC to be integrated in the future.

2.4 Summary

This chapter has presented the SSR/IFF emulator user requirements. These have been subdivided into functional requirements, HW requirements and requirements for future use of the target emulator. In the next chapter, the system will be broken down into subsystems, and each subsystem will consequently be analysed and described by translating the user requirements into technical engineering specifications.

3. Chapter 3: System Concepts and Requirements Allocation

The following chapter aims to analyse the high level user requirements described in the preceding chapter as a basis for creating an appropriate system breakdown structure for the SSR/IFF target emulator. Concept summaries of relevant aspects of each subsystem of the target emulator are provided where needed. Requirements derived from the concept summaries or directly from the user requirements are allocated to each subsystem. The aim of this systems engineering approach is to minimise the technical risks of the project, and to allow for proper system design, implementation and testing.

Very limited literature is available for research on SSR/IFF, because of the military use of this technology. As a result, most of the information is classified and thus not accessible to the public. The NATO document describing the SSR/IFF standard [2] and the classic SSR/IFF book by Stevens [1] were studied in depth, and have been used to derive the timing and operational requirements for SSR/IFF modes 1, 2, 3/A, C and secure mode 4.

The final section of this chapter is a traceability matrix, which maps the user requirements in the preceding chapter to their relevant derived requirements in this chapter. This ensures that all the user requirements have been considered.

3.1 User Requirements Analysis

The aim of the user requirements analysis is to examine the user requirements in the preceding chapter and to extract a system breakdown structure from them, which will also take into account any special considerations for the system design. Once the operational concepts of each subsystem in the structure have been explained, the requirements can be translated into engineering specifications.

The SSR/IFF target emulator system can be broken down into the subsystems depicted in Figure 3.1. The following points succinctly present the analysis.

1. The fact that user requirements exist for TxP and TCC emulation, reply modes and real-time operation shows that there is specific user interest in TxP and TCC operation and timing characteristics. Therefore, standalone TxP and TCC subsystems will be placed in the system breakdown structure.
2. Since the system is required to test an existing interrogator, even though there are no specific user requirements in respect of the interrogator, there are requirements for the implementation of FRUIT, which means that the system has to emulate the behaviour of multiple interrogator transmitters. Interrogator and ICC subsystems (for mode 4 FRUIT replies) will therefore be part of the system breakdown structure.
3. As the system must be able to generate FRUIT and garbled replies, a separate subsystem will be created for these.
4. Subsystems allocated for target identity and mobility will be created because of the user requirements for multiple targets, target mobility and distinct target identity (including the mode 4 friendly/non-friendly status). Requirements for information, which is necessary to maintain target identity existence and continuation in the simulated space, have to be allocated to these subsystems.
5. The system is required to operate in a continuous live mode and in real time, which must be taken into account when designing the necessary subsystems in order to accomplish these tasks. Consequently, subsystems will be created in respect of the requirements allocation for continuous and real-time operation.
6. The system is required to interface with an SSR/IFF antenna or to emulate one. The implication of this for the system and the requirements for an emulated antenna will be covered in the section that examines the target mobility subsystem.
7. The use of the Quixote board is a user requirement; therefore, it is unnecessary to conduct a study identifying a more suitable processor(s)/board; the results of this project will however indicate whether additional processing power is needed to meet the user requirements.

8. Finally, the requirements allocation for the ITRC interface, and general HW interfaces to the interrogator will be covered separately in the sections dealing with the HW and ITRC interface subsystem.

In Sections 3.4 to 3.14 below, each of the subsystems in Figure 3.1 will be studied and the relevant requirements for each of them will be identified and allocated.

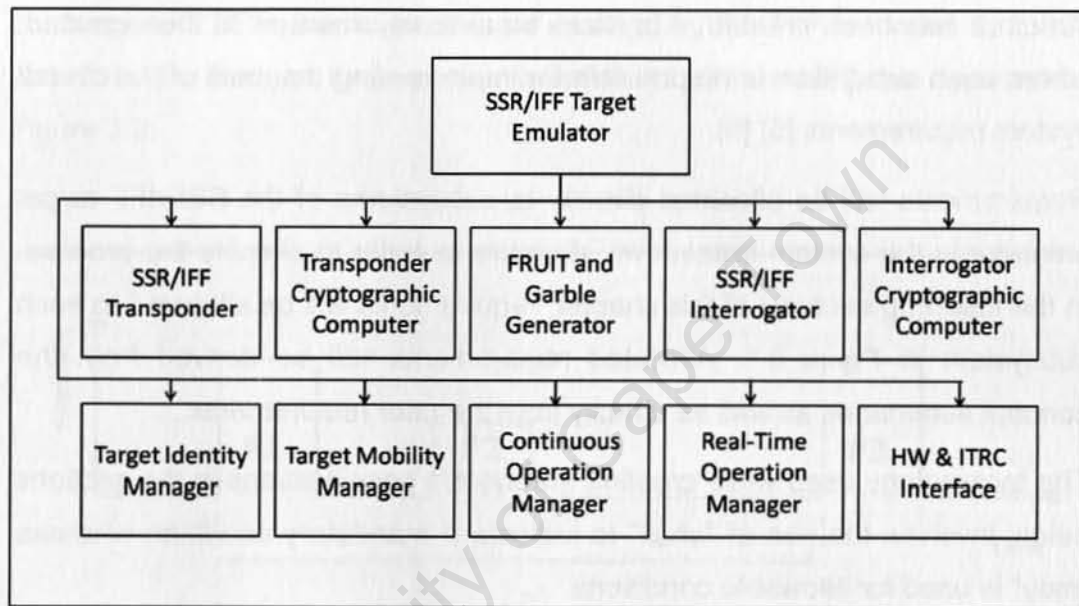


Figure 3.1 : SSR/IFF target emulator system breakdown structure. The figure presents the proposed subsystems of the SSR/IFF target emulator system.

3.2 Subsystem Concept Summaries Introduction

In order to understand the operational concepts of the subsystems in the system breakdown structure, a concept summary of the relevant aspects of the project will be presented in respect of each subsystem. For each individual requirement, a more detailed examination will be presented where needed.

The user requirements in the preceding chapter clearly stated that the system must comply with the timing requirements as set by the NATO document STANAG-4193 [2], and thus this document has been used as the source of most of the timing related analysis activities. Its use as a source of theoretical

SSR/IFF information has proven problematic however, because the authors of the document intended it to be a technical specification document for distribution to military equipment manufacturers rather than an academic document.

3.3 Requirements Allocation Introduction

In systems engineering, requirements are traditionally allocated to functions after a functional analysis has been performed, and a functional breakdown structure has been created. A system breakdown structure is then created, where each subsystem is responsible for implementing a subset of the overall system requirements [5] [6].

Requirements will be allocated directly to subsystems of the SSR/IFF target emulator in the system breakdown structure in order to simplify the process. In the following sections of this chapter, requirements will be allocated to each subsystem in Figure 3.1. Allocated requirements will be derived from the concept summaries as well as directly from the user requirements.

The terminology used while creating the system specifications in the sections below involves the use of “shall” to indicate a mandatory condition whereas “may” is used for allowable conditions.

3.4 TxP Concept Summary and Requirements

The subsections below present a concept summary for SSR/IFF TxP digital timing characteristics relevant to the system, followed by a listing of the requirements allocated to the emulated TxP.

3.4.1 SSR/IFF TxP Concept Summary

In order to meet the TxP specific user requirements, an analysis will be performed of the operational, functional and timing requirements of the SSR/IFF TxP, which are relevant to the system.

3.4.1.1 SSR/IFF Modes of Operation

There are currently 7 commonly used modes of operation in SSR/IFF, namely modes 1, 2, 3/A, C, 4, 5 and S. Military platforms typically use modes 1, 2, 3,

4 and 5, whereas civilian platforms typically use modes A, C and S [1]. Modes 1, 2 and 3 are known as Selectivity Identification Feature (SIF) modes [1]. Mode S is currently being used to replace SIF modes, although many countries around the world are still only using SIF modes. The target emulator will support SIF modes 1, 2, 3/A and C, and the secure mode 4.

3.4.1.2 SSR Non-Secure Modes

Pulses transmitted by the interrogator are known as interrogations, or challenges. In SSR, interrogations are received by the TxP in modes 1, 2, 3/A and C in the form of three pulses labelled P1, P2 and P3, as depicted in Figure 3.2.

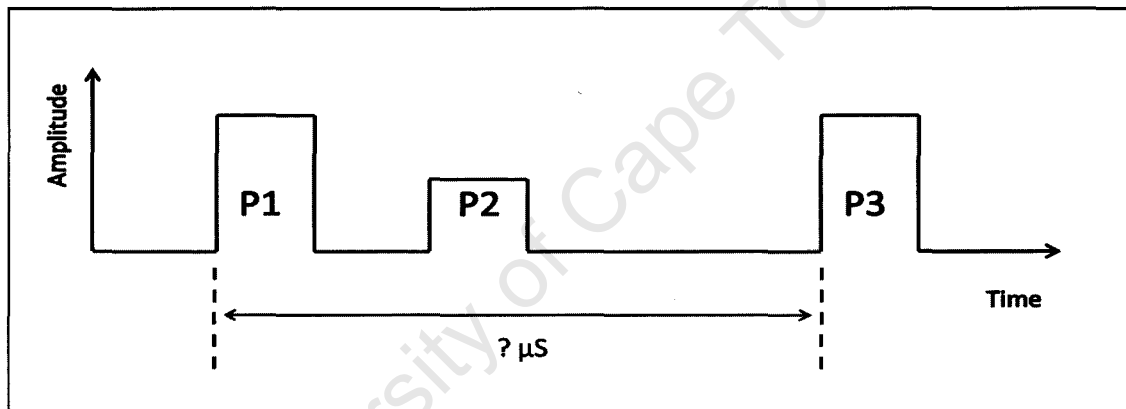


Figure 3.2 : From [1]. SSR interrogation signal format. The time duration between P1 and P3 determines the mode of the SIF interrogation.

The time interval between pulses P1 and P3 determine the interrogation mode, i.e. the type of information requested by the interrogator from the target TxP, as described in Table 3.1. Pulse P2 is the side-lobe suppression pulse and will be discussed in Section 3.4.1.4.

The military typically uses interrogations in modes 1 and 2 to request the target's identity and mission number; this can be assigned by the military agency in charge, and it can be set on the TxP by the target crew, captain or pilot prior to a mission [1] [4]. Mode 3/A is used in civil aviation for air traffic control purposes, and in the military for target identification. Mode C is

generally used in civil aviation to request the target altitude, which is reported by an altitude encoder (altimeter) connected to the TxP [1].

Table 3.1 : From [1]. Common SSR Interrogation Modes Summary

Interrogation Mode	P1 – P3 Spacing (μ s)	User
1	3	Military
2	5	Military
3/A	8	Military/Civil
C	21	Civil

SSR Replies:

The typical SSR reply format is shown in the figure below.

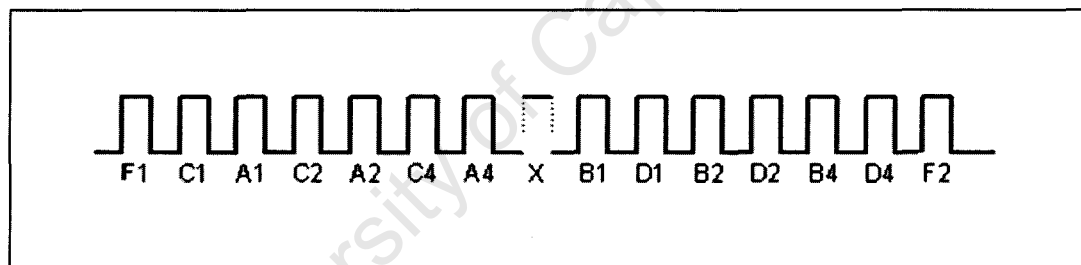


Figure 3.3 : General reply format of SSR SIF modes (adapted from [2]). The non-secure mode reply consists of a set of framing pulses called F1 and F2, which are always present in a reply [1]. Between these framing pulses are 13 data pulses. One of the pulses, labelled "X" is not used, leaving 12 data pulses and allowing for a maximum of 2^{12} (4096) possible reply code combinations [1].

Not all the data pulses illustrated in Figure 3.3 are necessarily used in all SSR modes [1]. Table 3.2 presents the designations of these pulses.

Table 3.2 : From [1]. SSR Data Pulses Designation

Interrogation Mode	Maximum Number of Possible Reply Combinations	Pulse Designations (see Figure 3.3)
1	32 codes	B4, C1, C2, C4 not used
2	4096	All 12 pulses
3/A	4096	All 12 pulses
C	2048	D1 not used

Translation of Mode C Replies:

Mode C replies are used to report the target altitude to the interrogator. An altitude encoder is typically connected to the TxP, providing it with the altitude information, which is then translated by the TxP into the appropriate mode C reply.

SSR SPI and Emergency Replies:

The ground interrogator operator is able to request the target pilot or captain to turn on a switch labelled SPI via an audio channel. The switch is routed to the TxP, and an identification of position reply (also known as a SPI reply), is then transmitted by the TxP. SPI is supported in modes 1, 2 or 3/A. In the case of mode 1, it is comprised of two consecutive replies separated by a fixed delay, as opposed to the normal single reply group. In the case of modes 2 and 3/A [1] an extra pulse is transmitted after the end of a reply group. In the past, when ATC controllers encountered visual problems with the PPI display when trying to track targets manually by checking replies, they would often ask specific pilots to identify themselves using an SPI reply [3].

Emergency replies in modes 1, 2 and 3/A indicate an emergency or hijack condition on the platform, and the emergency switch connected to the TxP can be set manually by the pilot or the captain. The result of the activation of this switch is the generation of a normal, single reply group, followed by three sets of framing pulses F1-F2 from the TxP. SPI and emergency replies are shown in Figure 3.4.

SSR Summary:

A summary of the timing characteristics of SSR modes 1, 2, 3/A and C is depicted in Figure 3.4. The interrogator side-lobe suppression (ISLS) in Figure 3.4 will be discussed in Section 3.4.1.4.

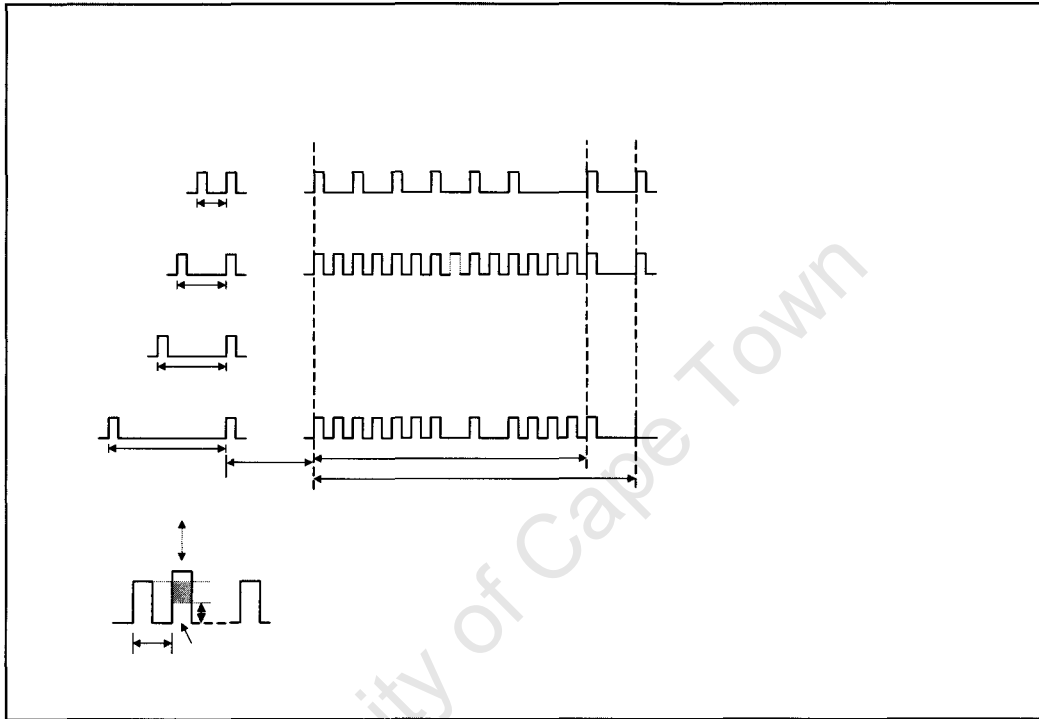


Figure 3.4 : From [2]. SSR Timing Diagram for Modes 1, 2, 3/A and C

3.4.1.3 IFF Secure Mode 4

Mode 4 is a method that enables the interrogator to determine a friendly target with certainty. Added security measures have been built into the challenge/response mechanism in mode 4, which hinder a foe target's ability to copy the identity of a friendly target in a non-secure mode. These mechanisms leave very little room for an identification error.

A secure mode 4 interrogation received by the TxP differs from non-secure modes in that it comprises thirty-seven pulses as opposed to three, as seen in Figure 3.5 and Figure 3.8. The first four pulses are known as the "Sync Pulse Group" [2], whereas the fifth pulse is the side-lobe suppression pulse, as will

be discussed in Section 3.4.1.4 below. The following 32 pulses consist of an encrypted message generated by the ICC. The message contains the reply delay value for which the TxP must wait, before producing a mode 4 reply; this is in the form of three pulses, as seen at the bottom of Figure 3.8.

If a target produces a certain number or percentage of delayed replies, which correspond correctly to the decrypted values in the received challenges, the interrogator will declare that target a friend. As a result, the target will be plotted as a friend on the radar display.

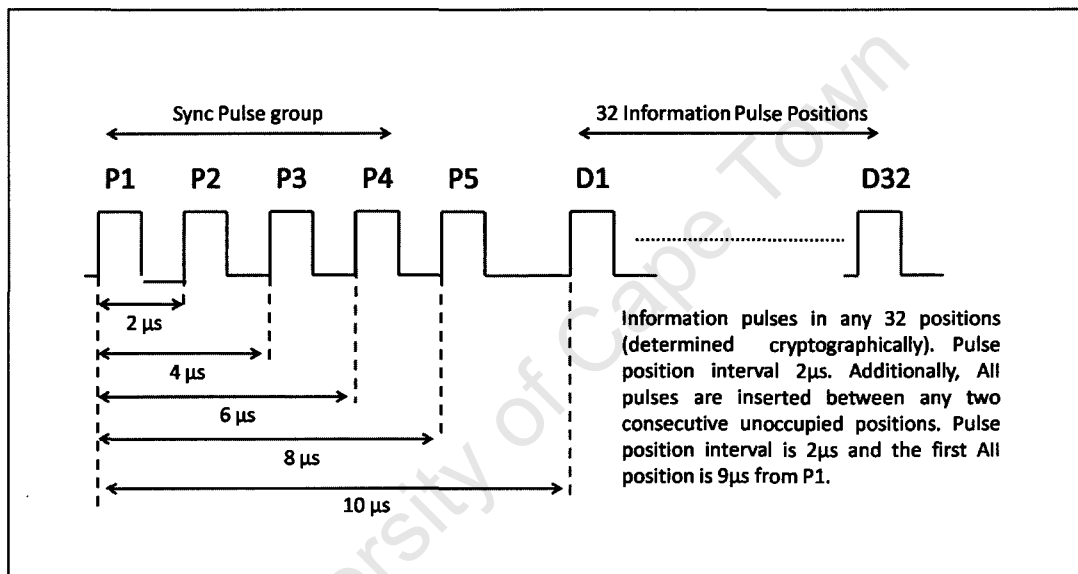


Figure 3.5 : Adopted from [2]. IFF secure mode 4 challenge timing diagram. Anti Interference Interrogation (All) pulses will be covered in the following subsection

The abovementioned reply delay value is added to a fixed delay value, the total value of which the TxP must wait before it may produce a reply. This fixed delay allows the TxP enough time to pass on the challenge to the TCC attached to it, as shown in Figure 1.1, and it furthermore allows time for the TCC to decrypt the challenge. This delay mechanism further allows the interrogator to validate the target range accurately, which is done based on the exact time when the reply was received from the target, as illustrated in Figure 3.6. The secure mode 4 reply comprises a set of three pulses, as shown in Figure 3.6 and Figure 3.8, although these have no data significance. The important issue is the correct timing [3].

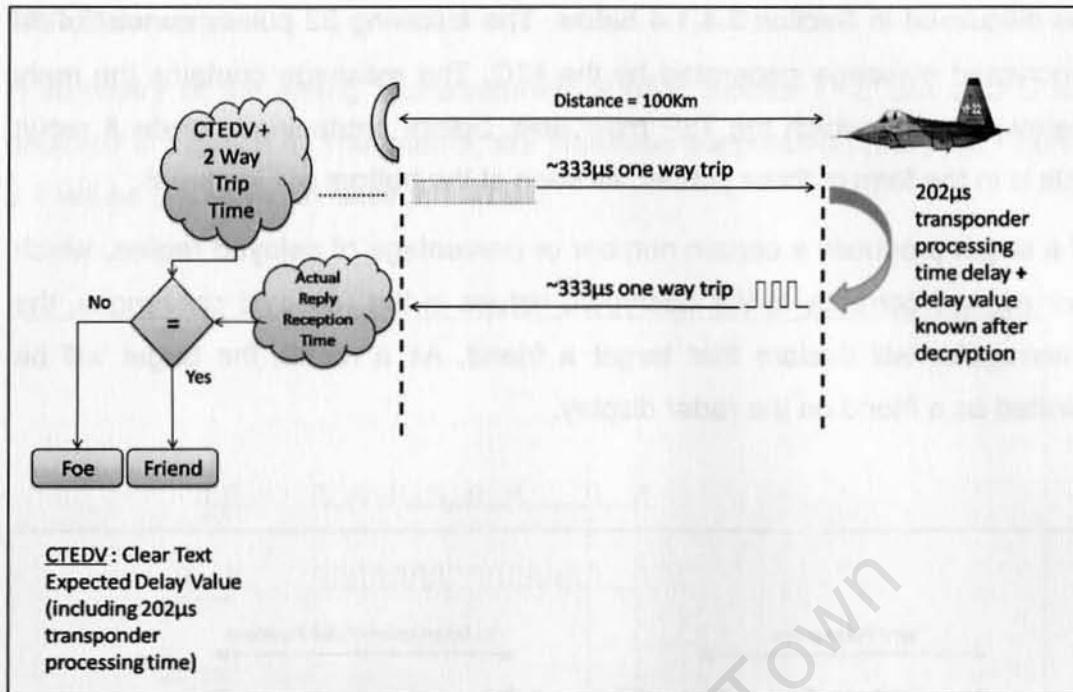


Figure 3.6 : Example of secure mode 4 reply validation algorithm. As the interrogator antenna rotates, and as the target is illuminated in the beam, the scenario in the figure may repeat several times, based on factors such as the beam width, the target speed, the antenna rotation period, the range of the target and the PRF of the interrogator. The number of times the above operation needs to happen before a target is declared a friend is dependent on the interrogator design.

Anti Interference Interrogation (All) Pulses:

The 32 pulses or pulse positions may not always be used, as whether they are used or not is dependent upon the value of the encrypted message. STANAG-4193 [2] specifies that All pulses must be "inserted between any two adjacent unoccupied pulse positions of the information pulse group" [2].

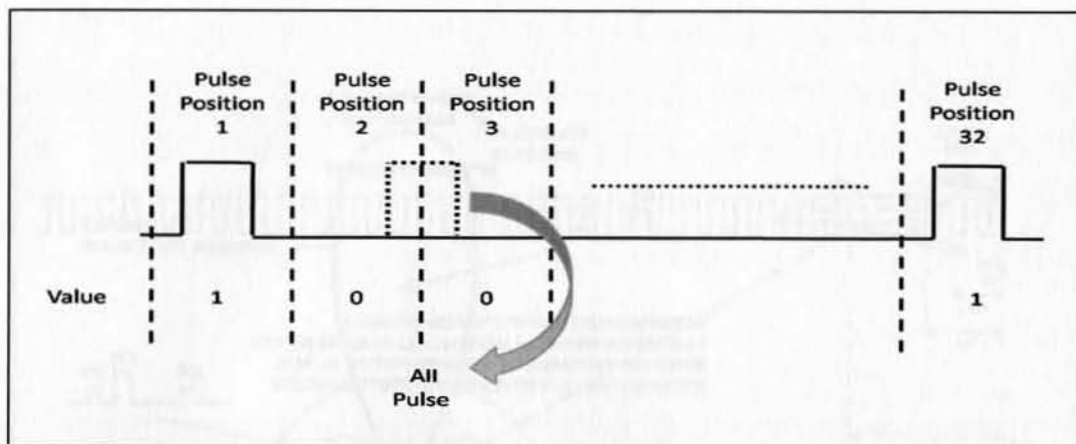


Figure 3.7 : Secure mode 4 All pulse scenario. All pulses are inserted between any two adjacent unoccupied pulses in the encrypted interrogation.

Mode 4 Summary:

A summary of the secure mode 4 and its timing characteristics is presented in Figure 3.8 below.

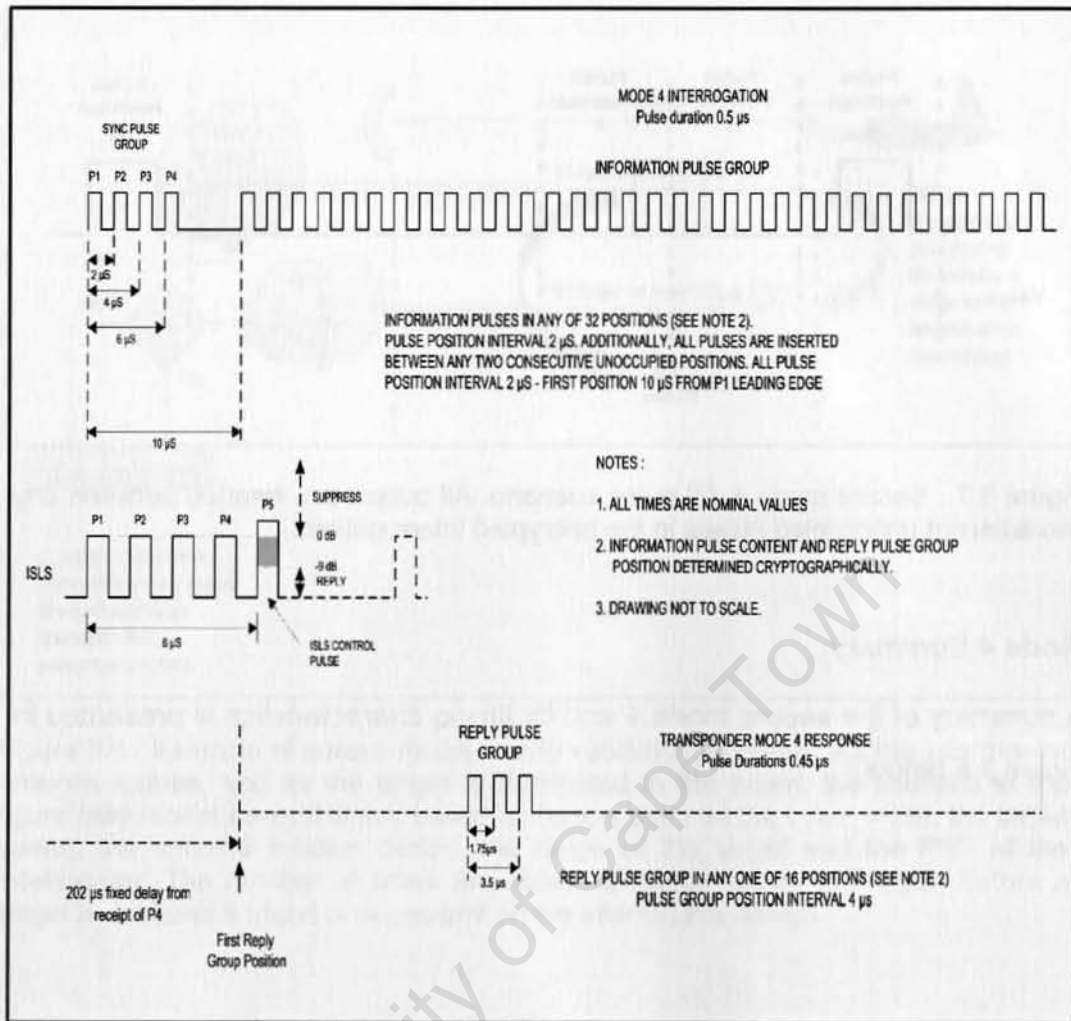


Figure 3.8 : From [2]. IFF timing diagrams for secure mode

3.4.1.4 Interrogator Side-lobe Suppression

Interrogator antenna patterns are not perfect and may have undesirable side-lobe radiation patterns [2], [3]. TxPs do not reply if they are located in the side-lobes of the antenna as that may cause the interrogator to presume falsely that a target is present in the direction of the main beam. A side-lobe suppression pulse is thus transmitted with a higher amplitude by a separate antenna of the interrogator in the side-lobes to inform TxPs that they are located in the side-lobes and should not reply to received interrogations. This is known as Interrogator Side-Lobe Suppression (ISLS) [2].

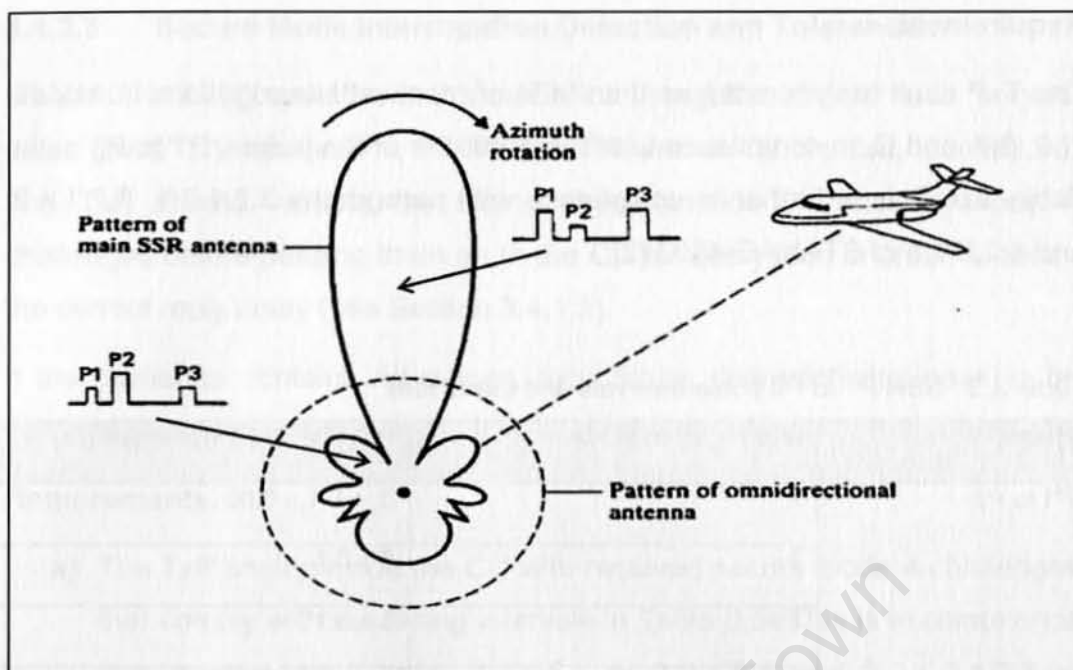


Figure 3.9 : From [3]. SSR/IFF interrogator antenna patterns. If a target is in the main antenna beam, it will receive a P2 pulse of an amplitude that is lower than that of P1 and P3, and it should therefore reply to the received interrogation. For the secure mode 4, pulse P5 is designated as the side-lobe suppression pulse.

An interrogator, with an antenna arrangement as in Figure 3.9 for modes 1, 2, 3/A and C, transmits pulses P1 and P3 using the main directional antenna, whereas P2 is transmitted via the separate omnidirectional antenna. In secure mode 4, pulse P5 is the side-lobe suppression pulse and it is transmitted by the omnidirectional antenna. In the mode 4 interrogation, pulse P2 is transmitted with the directional antenna to suppress TxPs, which are not enabled to reply in mode 4. The location of P5 in the secure mode 4 interrogation is presented in Figure 3.5 and Figure 3.8.

3.4.2 SSR/IFF TxP Requirements

The following subsections discuss the requirements allocation in respect of the emulated SSR/IFF TxP subsystem.

3.4.2.1 Non-Secure Interrogation Mode Detection and Tolerance

The received interrogations in modes 1, 2, 3/A, and C are detected based on the time interval between the pulses P1 and P3 (see Figure 3.4 above).

Requirement:

The TxP shall reply to not less than 90% of received interrogations in modes 1, 2, 3/A and C, in compliance with the durations of the pulses P1 to P3 as in Table 3.3. This is further in compliance with paragraphs 3.2.1.3.1, 3.2.1.3.2 and 4.2.5.1.a of STANAG-4193 [2].

Table 3.3 : SSR P1 to P3 pulse intervals and tolerances

Pulse(s)	Interrogation Mode	Interval and Tolerances (μ s)
P1 to P3	1	$3 + 0.1, - 0.05$
	2	5 ± 0.1
	3/A	8 ± 0.1
	C	21 ± 0.1
P1 to P2	1, 2, 3/A and C	$2 + 0.5, - 0.15$

3.4.2.2 Non-Secure Modes Interrogation Pulse Width Validation

STANAG-4193 [2] requires the TxP to validate the pulse widths of received interrogations before replying to them.

Requirement:

The TxP shall validate the width of received interrogation pulses against the durations in Table 3.4. This is in compliance with paragraphs 3.2.1.2, 4.2.5.1.b and 4.2.6.3.1 of STANAG-4193 [2].

Table 3.4 : SSR interrogation pulses duration and tolerance

Pulse(s)	Duration and Tolerance (μ s)
P1 and P3	0.8 ± 0.1
P2	$0.8 + 0.05/- 0.1$

3.4.2.3 Secure Mode Interrogation Detection and Tolerance

STANAG-4193 [2] specifies that a mode 4 interrogation should have "a sync-pulse group" [2], labelled P1, P2, P3 and P4, and an ISLS pulse, labelled P5. The TxP should validate the timing characteristics of received mode 4 challenges before passing them on to the CC for decryption in order to obtain the correct reply delay (see Section 3.4.1.3).

If the challenge contains All pulses, their timing characteristics have to be validated.

Requirements:

- a) The TxP shall provide the CC with received secure mode 4 challenges that comply with the timing intervals in Table 3.5. This is in compliance with paragraphs 3.2.1.4, 3.2.1.5.1 to 3.2.1.5.4 and 3.2.1.2.4.2.2 of STANAG-4193 [2].
- b) The timing of All pulses "inserted between any two adjacent unoccupied pulse positions of the information pulse group" [2] shall be validated.
- c) The challenges provided to the CC shall include the P3, P4 and P5 pulses, and the following 32 information pulse group shall include the All pulses, in compliance with paragraph 4.2.5.2.1 of STANAG-4193 [2].

Table 3.5 : IFF Secure Mode 4 Pulse Intervals and Tolerances

Pulses	Interval and Tolerance (μ s)
P1 to P2	2 ± 0.1
P1 to P3	4 ± 0.1
P1 to P4	6 ± 0.1
P1 to P5	8 ± 0.1
Combined relation between P1, P2, P3 and P4	Not greater than 0.6 from their normal intervals
P1 to first information pulse D1	10 ± 0.1

Pulses	Interval and Tolerance (μs)
D1 to D32	± 0.1 with respect to P1
P1 to First All (if applicable)	9 ± 0.1
P1 to any All	odd multiples of 1 ± 0.1

3.4.2.4 Secure Mode 4 Interrogation Pulse Width Validation

The TxP should validate the pulse widths of received secure mode 4 challenges before passing them on to the CC for decryption.

Requirement:

In compliance with paragraphs 3.2.1.4, 4.2.5.2.1 and 4.2.6.3.2 of STANAG-4193 [2], the TxP shall validate the pulse widths of received mode 4 challenges against the timing information in Table 3.6.

Table 3.6 : IFF secure mode 4 pulse durations

Pulse(s)	Duration and Tolerance (μs)
P1 to P5	0.5 ± 0.1
D1 to D32 information group and All pulses	0.5 ± 0.1

3.4.2.5 Enable Trigger Signal Generation

A secure mode 4 interrogation received by the TxP will be passed to the CC connected to it. The enable trigger signal informs the CC that a challenge is going to be passed to it for decryption (see Figure 3.10).

Requirement:

The TxP shall generate an enable trigger signal to the TCC in compliance with the timing in Table 3.7, if a valid secure mode 4 challenge is received. This is in compliance with paragraphs 1.2.6 and 4.2.5.2.2 of STANAG-4193 [2].

Table 3.7 : Mode 4 enable trigger timing and tolerance

Description	Time and Tolerance (μ s)
Enable Trigger Pulse Position	0.45 ± 0.05 after P4
Enable Trigger Pulse Duration	0.5 to 3.0

3.4.2.6 Interrogator Side-lobe Suppression

TxPs in the antenna side-lobes of the interrogator receive side-lobe suppression pulses with greater amplitude than other pulses in the interrogation group; this should prevent TxPs from replying to such interrogations (Section 3.4.1.4).

Requirements:

- a) In compliance with paragraphs 2.2.3, 3.2.3, 4.2.7.1, 4.2.7.2 of STANAG-4193 [2], the TxP shall not reply to more than 10% of valid interrogations received in modes 1, 2, 3/A and C if a P2 side-lobe suppression pulse is valid (according to the interrogation group timing specifications as set out in Sections 3.4.2.1 and 3.4.2.2). This is also applicable to a P5 side-lobe suppression pulse in secure mode 4 according to the timing specifications in Sections 3.4.2.3 and 3.4.2.4.
- b) The TxP suppression period shall be as brief as possible, and shall not exceed 35 μ S, in compliance with paragraphs 4.2.8.4.2 and 4.2.8.4.3 of STANAG-4193 [2].

3.4.2.7 TxP Internal Suppression

When the TxP decodes a correct interrogation, it must not accept any new incoming interrogations, valid or invalid, for the time needed to produce a reply to the first interrogation for modes 1, 2, 3/A, C and 4 [2].

Requirements:

- a) In compliance with paragraphs 4.2.11 and 4.2.11.1 from STANAG-4193 [2], the TxP shall not decode incoming interrogations if a valid interrogation has been decoded until the appropriate reply has been produced.

- b) For modes 1, 2, 3/A and C, the TxP shall be able to process the first pulse of an incoming interrogation within 10 μ S of the completion of the reply.
- c) For mode 4, the TxP shall be able to process the first pulse of an incoming interrogation within $290 \pm 10 \mu$ S unless the reply is produced before such time, in compliance with paragraph 4.2.11.2.b of STANAG-4193 [2].

3.4.2.8 Non-secure Modes Replies

A mode 1, 2, 3/A or C reply generated by the TxP after receiving a valid interrogation consists of a pair of framing pulses, namely F1-F2. The data pulses between F1 and F2 are relevant to the reply mode and the reply code. It is important to follow the reply timing characteristics by the TxPs in order to ensure that the interrogator will accept and identify the replies.

Requirements:

- a) The replies produced by the TxP in modes 1, 2, 3/A and C shall comply with the timing characteristics in Table 3.8. This is in compliance with paragraphs 4.3.1.2, 4.3.1.3, 4.3.1.3.1 and 4.3.1.3.2 of STANAG-4193 [2].

Table 3.8 : Non-secure modes reply timing characteristics

Description	Interval and Tolerance (μ s)
Reply Group Pulse Duration	0.45 ± 0.1
F1 to F2 interval	20.3 ± 0.1
Pulse Interval Tolerance for Each Pulse with Respect to F1	± 0.1
Pulse Interval Tolerance for Each Pulse with Respect to any other Pulse Except F1	± 0.15

- b) The reply group data pulses produced by the TxP shall follow the timing as set out in Table 3.9 with respect to the first framing pulse F1, in compliance with paragraph 4.3.1.3.2 of STANAG-4193 [2].

Table 3.9 : From [2]. Non-secure modes reply pulse positions from F1

Pulse	Nominal Position (μ s)
C1	1.45
A1	2.90
C2	4.35
A2	5.80
C4	7.25
A4	8.70
X	10.15
B1	11.60
D1	13.05
B2	14.50
D2	15.95
B4	17.40
D4	18.85

- c) In compliance with paragraph 4.3.1.3.3 of STANAG-4193 [2], the TxP reply shall "consist of four digits each of which lie between 0 and 7 inclusive and consist of the sum of the subscripts of the corresponding pulses employed"[2], following the designations in Table 3.10 and Table 3.11.

Table 3.10 : From [2]. Modes 1, 2, 3/A and C reply code designation

Digit	Pulse Group
First	A (A1, A2, A4)
Second	B (B1, B2, B4)
Third	C (C1, C2, C4)
Fourth	D (D1, D2, D4)

Table 3.11 : From [2]. Modes 1, 2, 3/A and C employed reply pulses

Mode	Pulses Employed
1	A1, A2, A4, B1 and B2
2	A, B, C and D
3/A	A, B, C and D
C	All pulses A, B, C and D, except D1

3.4.2.9 Non-secure Modes SPI and Emergency Replies

As described in the above subsection 3.4.1.2, platforms fitted with a TxP may be asked to produce SPI replies. Alternatively, the platform pilot or captain can choose to produce an emergency reply, which indicates to the interrogator that there is an emergency condition.

Requirements:

- a) An SPI reply for mode 1 shall consist of a normal reply, followed by a repetition of that reply starting at an interval of $24.65 \pm 0.1 \mu\text{s}$ from the first framing pulse of the first reply, with a tolerance of $\pm 0.1 \mu\text{s}$ from the first framing pulse of the first reply, and $\pm 0.15 \mu\text{s}$ to any other pulse in the reply, in compliance with paragraph 4.3.1.6.1 of STANAG-4193 [2].
- b) An SPI reply in modes 2 and 3/A shall consist of the normal reply followed by a single pulse at an interval of $24.65 \mu\text{s}$ with a tolerance of

$\pm 0.1 \mu\text{s}$ from the first framing pulse of the first reply group, in compliance with paragraph 4.3.1.6.2 of STANAG-4193 [2].

- c) An emergency reply in modes 1, 2 and 3/A shall consist of a normal reply group followed by three sets of framing pulses F1-F2 (empty replies) according to the timing in Table 3.12, in compliance with paragraph 4.3.1.7.1 of STANAG-4193 [2].
- d) The emergency reply code in mode 3/A shall be 7700 and shall override any preselected selected mode 3/A code, in compliance with paragraph 4.3.1.7.3 of STANAG-4193 [2].

Table 3.12 : From [2]. emergency reply groups timing from first reply F1

Emergency Empty Reply Group Number	F1 Pulse (μs)	F2 pulse (μs)
2	24.65 ± 0.1	44.95 ± 0.1
3	49.30 ± 0.1	69.60 ± 0.1
4	73.95 ± 0.1	94.25 ± 0.1

3.4.2.10 Secure Mode 4 Reply

When the TxP receives a secure mode 4 challenge and validates the timing characteristics thereof, it passes that challenge to the attached CC for decryption. If the CC successfully decrypts the challenge, it will inform the TxP of the delay value in microseconds. This delay value is reported back from the CC, which is added to a fixed $202 \mu\text{s}$ delay, the value of which the TxP must wait for before producing a three pulses reply group as in Figure 3.6 and Figure 3.8. The delay value reported back from the CC can only be one of sixteen possible delay values starting from 0 to $60 \mu\text{s}$ in multiples of four.

Requirements:

- a) The TxP shall produce a reply pulse group consisting of three pulses with timing characteristics as in Table 3.13, in compliance with

paragraphs 4.3.1.2, 4.3.1.4, 4.3.1.5, 4.3.1.5.1 and 4.3.1.5.2 of STANAG-4193 [2].

- b) The TxP shall have a means of communicating challenges and replies to the TCC (described in Section 3.5 below).

Table 3.13 : IFF secure mode 4 reply timing characteristics

Description	Time and Tolerance (μs)
Reply Group Pulses Width	0.45 ± 0.1
P1 to P2 interval	1.75 ± 0.05
P1 to P3 interval	3.5 ± 0.05
Reply Group Position (from reception of P4 pulse of the challenge)	$199.5 \pm 0.75 + \text{CC Reported Delay}$

3.4.2.11 Non-Secure Modes Reply Delay

All STANAG-4193 [2] compliant TxPs have fixed reply delays in respect of modes 1, 2, 3/A and C, which are measured from the reception of the last interrogation pulse. The reason for this is to allow the different TxP manufacturers to process received interrogations at their own pace, provided it does not take longer than the specified delay. Interrogators use this fixed reply delay to determine the range of the replying platform, with an inaccuracy of R_x being:

$$R_x = (C \times T_{to})/2 \quad (3.1)$$

Where C is the pulse propagation time, which in radar is the speed of light in a vacuum (299792458ms^{-1}) [12], whereas T_{to} is the delay tolerance specified below of $\pm 0.5 \mu\text{S}$. This leads to the tolerance R_x being approximately equal to 75m, which equates to an uncertainty in range of approximately 150m ($75\text{m} \times 2$).

Requirement:

The TxP reply delay for modes 1, 2, 3/A and C shall be 3.0 μ s with a tolerance of $\pm 0.5 \mu$ s from the rising edge of the interrogation pulse P3 to the rising edge of the reply pulse F1, in compliance with paragraph 4.3.4.1 of STANAG-4193 [2].

3.4.2.12 Secure Mode 4 Processing Delay

The concept applied in Section 3.4.2.11 in respect of the non-secure modes can be similarly applied for mode 4, but a longer delay is allowed to enable the TxP to pass the challenge to the TCC for decryption (see Figure 3.6). However, this must not be confused with the reply delay induced by the TxP TCC, which is discussed in Section 3.5.2.4 below.

Requirement:

The TxP reply delay for mode 4 shall be 202 μ s with a tolerance of $\pm 1.25 \mu$ s from the rising edge of the interrogation pulse P4 to the rising edge of the first pulse of the mode 4 reply, in compliance with paragraph 4.3.4.2 of STANAG-4193 [2].

3.4.2.13 TxP Reply Rate**Requirement:**

The TxP shall have a reply rate capability of 1200 replies per second, in compliance with paragraph 4.3.5 of STANAG-4193 [2].

3.4.2.14 TxP Video Signal Sampling

The TxP timing specifications discussed in the subsections above generally call for signal tolerance measurements in hundreds of ns, and may be as low as 50 ns, as explained in Section 3.4.2.2, for example. Using a 40 MHz clock will allow for proper sampling of the signals since it is twice the maximum frequency.

Requirement:

The system shall be able to sample the digital video signals at a speed of at least 40 MHz.

3.4.2.15 Reply Mode Enable/Disable Selectivity

Requirement:

The TxP shall allow for an enable/disable input switch, which either enables or disables the replies in a specific interrogation mode.

3.5 TCC Concept Summary and Requirements

As depicted in Figure 3.1, the emulation of IFF TCCs is necessary to emulate secure mode 4 replies.

3.5.1 IFF TCC Concept Summary

To meet the relevant aspects of the user requirements, the following subsections analyse the related operational and functional characteristics of the IFF TCCs, as well as the timing requirements, to which the system must adhere. These have been compiled using STANAG-4193, with specific reference to Appendix 3 of Annex A [2]. For the sake of completeness, selected secure mode 4 TCC related topics have been covered under the TxP concept summary.

3.5.1.1 The Operation of IFF TCCs

The SSR/IFF TxP as described in Section 3.4 is capable of receiving and identifying a secure mode 4 encrypted interrogation, which it passes on to the TCC for decryption. The IFF secure mode 4 summary contained in Section 3.4.1.3 and illustrated in Figure 3.8 depicts the correct delay or waiting time of the TxP before it generates a standard three-pulse reply, which its value is embedded in the challenge and encrypted. If the challenge is successfully decrypted by the TCC, the TCC will inform the TxP of the value of that delay. The delay can be one of sixteen possible values, as contained in the specification for the secure mode 4 reply in Section 3.4.2.10.

The target carrying the TxP and TCC may be considered a foe by the interrogator generating the challenges if the TxP does not generate correct replies to a certain percentage (as determined by the interrogator) of the overall number of challenges received due to the following reasons:

- Failure of the decryption process in the TCC.

- The decryption process exceeding the maximum time specified by STANAG-4193 [2] to decrypt the challenge in the TCC.

3.5.1.2 TCC-TxP Operation Sequence

Figure 3.10 shows the process of signalling and timing when an IFF mode 4 challenge is being passed to the TCC with a request to decrypt from the TxP. The mode 4 interrogation challenge characteristics shown in Figure 3.5 are still applicable to this process.

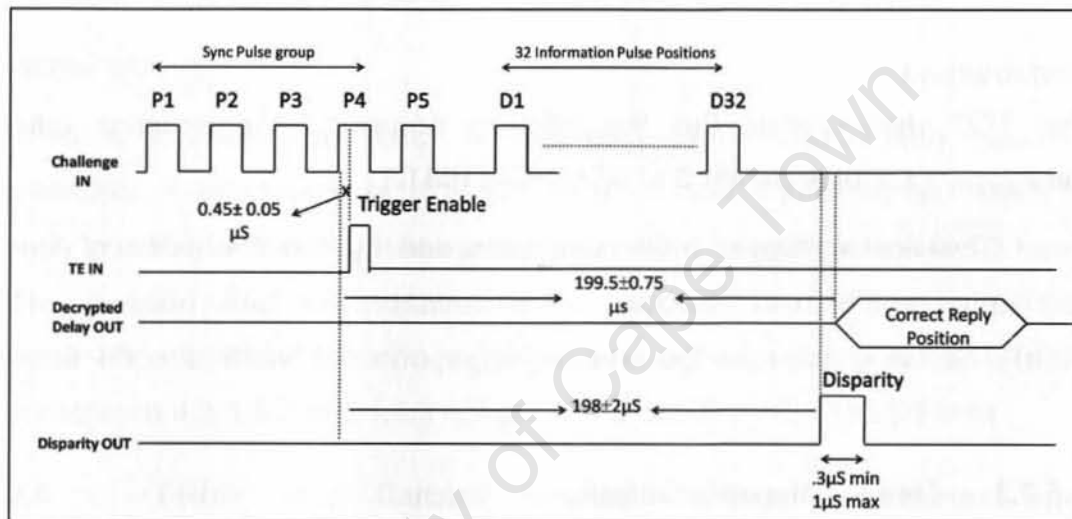


Figure 3.10 : IFF secure mode 4 interrogation decryption sequence. The TCC receives the challenge from the TxP, and if a trigger enable signal is present during the period of the pulse P4, the TCC must attempt to decrypt and provide the decryption result in a time less than $199.5 \pm 0.75 \mu\text{s}$. The decryption result is a replay delay as described in Section 3.4.1.3. The TCC must produce a disparity pulse if the challenge decryption has failed.

3.5.2 IFF TCC Requirements

The following subsections present the requirements allocated to the emulated IFF TCC.

3.5.2.1 TCC Processing Rate

Requirement:

The maximum number of IFF challenges that the TCC shall process is 3000 challenges per second, which is in compliance with paragraph 1.6.3 of Appendix 3 of STANAG-4193 [2].

3.5.2.2 Mode 4 Enable Trigger

The enable trigger signal is generated by the TxP to inform the TCC that it must process the challenge being passed to it, as seen in Figure 3.10.

Requirement:

The TCC shall validate that the following occurred, in compliance with paragraph 1.6.2 of Appendix 3 of STANAG-4193 [2]:

- a) The enable trigger pulse was preceded by the P4 pulse of the challenge by $0.45 \pm 0.05 \mu\text{s}$.
- b) The rising edge of the enable trigger occurred within the P4 time period.

3.5.2.3 Mode 4 Disparity Output

The TCC must generate what is known as a 'late disparity pulse' upon failure of the decryption of a mode 4 interrogation. Paragraph 1.7.2.1 of Appendix 3 of STANAG-4193 [2] calls for an early disparity pulse, which is generated, for example, in the presence of a P5 pulse or an All pulse error in the challenge. However, the emulated TCC will not have to implement such an early disparity pulse since the emulated TxP (specified in Section 3.4) is able to validate mode 4 challenges, including side-lobe suppression situations and All pulse errors.

Requirements:

- a) The duration of the disparity signal output from the TCC to the TxP shall have the minimum and maximum duration of $0.3 \mu\text{s}$ and $1 \mu\text{s}$ respectively, in compliance with paragraph 1.5.1 of Appendix 3 of STANAG-4193 [2].

- b) The disparity signal shall occur $198 \pm 2 \mu\text{s}$ after the occurrence of the rising edge of the enable trigger pulse, as described in Section 3.4.2.5, in compliance with paragraph 1.5.1 of Appendix 3 of STANAG-4193 [2].

3.5.2.4 TCC Mode 4 Processing Time and Reply Delay

When the TCC is requested to decrypt a received mode 4 challenge and to provide the reply position embedded in the challenge, it should do so within a certain time frame. The TxP requirements listed under Section 3.4.2.10 must be taken into consideration when examining the requirements below.

Requirement:

When a successful decryption is performed, the decrypted reply value is measured in microseconds, starting from $0 \mu\text{s}$ to $60 \mu\text{s}$, which represents a reply position in one of sixteen possible positions in multiples of $4 \pm 0.1 \mu\text{s}$. This position shall be available to the TxP $199.5 \pm 0.75 \mu\text{s}$ after the occurrence of the P4 interrogation pulse rising edge, in compliance with paragraphs 4.3.1.5.2 and 4.4.3 of Appendix 3 of STANAG-4193 [2].

3.6 FRUIT and Garbled Replies Concept Summaries and Requirements

For the system to generate FRUIT and garbled replies, according to the user requirements set out in Chapter 2, it is necessary to understand how these replies occur. The concept summaries below explore the role played by the existence of multiple interrogators in the region near the interrogator being tested, and the role played by multiple targets in FRUIT and garbling situations. Thereafter, the FRUIT and garble manager requirements are allocated.

3.6.1 FRUIT Replies Concept Summary

In SSR/IFF interrogator systems, FRUIT occur when a number of interrogators operate in close proximity to each other [3] [4]. In such a situation, TxPs generate replies, which are received and considered as FRUIT by other interrogators because they were not expected, i.e. they were not

responses to their own interrogations. FRUIT replies not identified as FRUIT may indicate targets at incorrect ranges [3] [4]. FRUIT is applicable to all the SSR/IFF interrogation modes supported by the target emulator.

Because of the arrival of asynchronous FRUIT replies, the interrogator signal processor should be able to "de-FRUIT" those replies to a certain extent, as specified by STANAG-4193 [2], to be around 20,000 FRUIT replies per second [2]. The term de-FRUIT in the context of STANAG-4193 [2] refers to an interrogator function, which de-correlates the FRUIT replies and prevents them from being identified as real targets. Interrogators can use different techniques to de-FRUIT replies, such as staggering the PRI or keeping track of a number of previous target replies. Figure 3.11 shows an example of FRUIT replies to which SSR/IFF interrogators may be exposed.

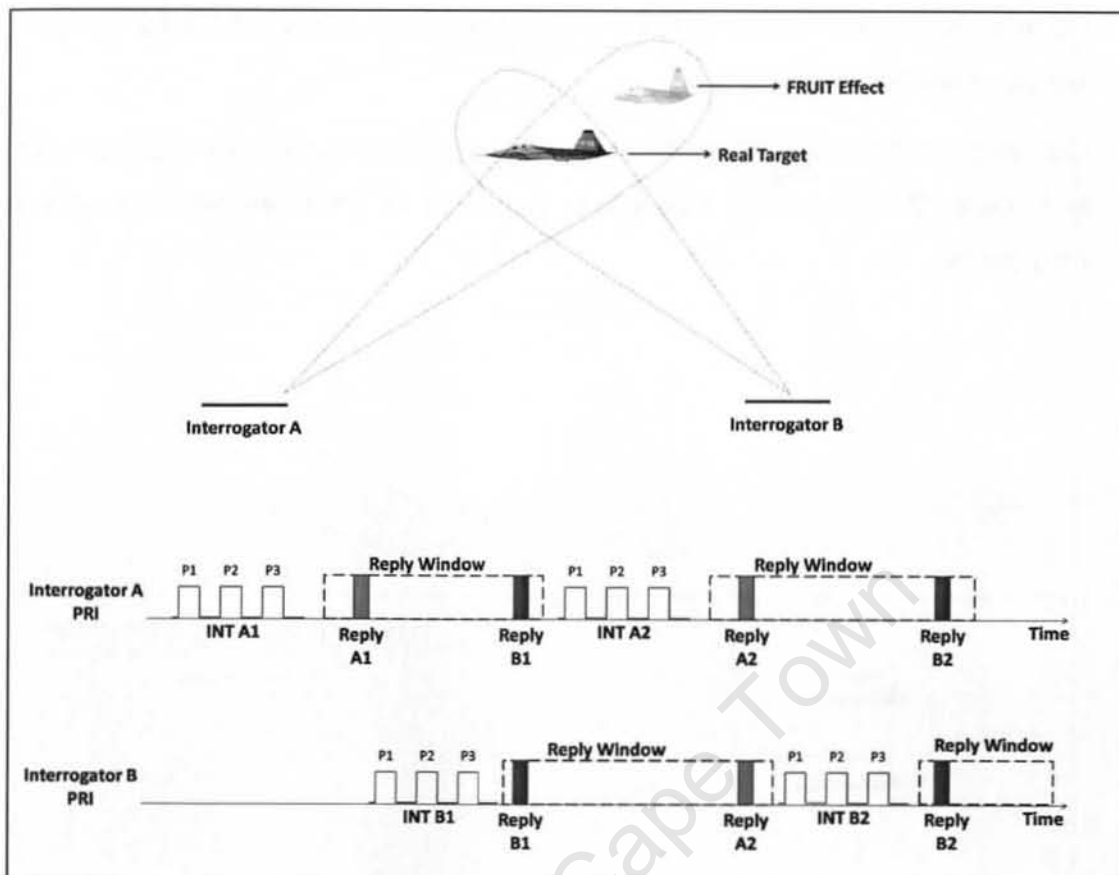


Figure 3.11 : Example of a FRUIT situation in SSR/IFF. Interrogator A and B operate at different PRF rates and are located in close proximity to each other. It is assumed that the interrogators have a fixed direction antenna or that they happen to be rotating in a manner that allows their beams to illuminate a target at the same time. The reply B1 to interrogation B1 will cause a FRUIT effect to be seen by interrogator A, and if interrogator A did not have de-FRUIT facilities, it will assume that there is a target at a further range from the actual target over a number of PRFs. The same applies to reply A2 being seen by interrogator B for only the first PRF. This does not apply to reply A1 to interrogation A1, however, as the reply receive window for interrogator B was closed when the reply A1 was generated.

3.6.2 Garbled Replies Concept Summary

In SSR/IFF, garbled replies occur when TxP replies from two or more targets overlap in time, which may cause ambiguity in their decoding process at the interrogator [2] [3]. Garbling occurs when two targets are at the same or at a close radial range from the interrogator, but at different altitudes [3]. The time tolerance allowed by STANAG-4193 [2] for TxPs to produce a reply also influences the ambiguity of the interpretation of the replies when targets are

close to each other (for example, the tolerance can be $\pm 0.1 \mu\text{s}$ for the SIF modes, see Section 3.4.2.11).

Garbling can happen in all SSR/IFF modes specified by the user requirements in Chapter 2. Figure 3.12 shows two examples of situations where garbling may occur.

University of Cape Town

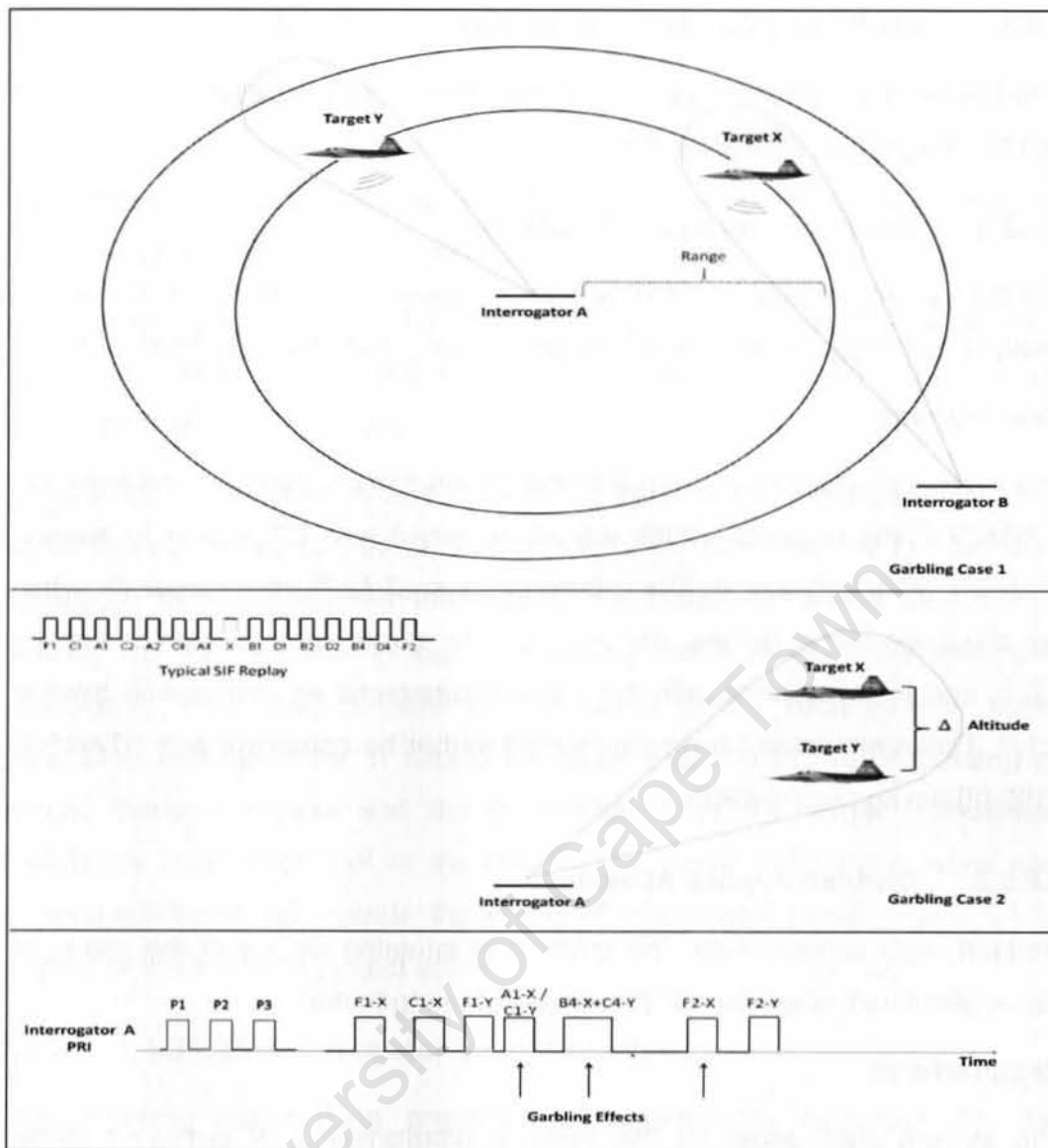


Figure 3.12 : Examples of garbling. In case 1, interrogator A is busy interrogating the sector containing target Y, but at the same time interrogator B is interrogating the sector containing target X, which happens to be at the same radial distance from interrogator A as target Y. The replies from target X to interrogations from interrogator B may be received by the side-lobes of interrogator A antenna, and these will then overlap with the replies from target Y. De-garble and de-FRUIT facilities in interrogators should handle problems like this over a number of replies and as the targets vary in range.

In case 2, two targets are also at the same range from interrogator A, but they are at different altitudes, which will result in an overlap in their replies.

The challenge-reply at the bottom of the figure is an example of what the overlapping in the replies would look like in both cases. Replies may overlap on a pulse-by-pulse level, thus resulting in wide pulses, like pulse B4 from target X combined with pulse C4 from target Y; alternatively, the ambiguity could result from trying to identify which pulses belong to which F1-F2 reply group. For instance, the pulse following F1-Y could be A1 from target X or C1 from target Y.

3.6.3 FRUIT and Garble Requirements

The following subsections present the requirements allocation in respect of FRUIT and garble reply generation.

3.6.3.1 Multiple Interrogator Emulation

For the system to create FRUIT replies, it needs to emulate the existence of multiple interrogators operating in close proximity and causing FRUIT effects.

Requirement:

The system shall be able to emulate the generation of interrogations from 0 to 2 SSR/IFF interrogators, which are all equipped with ICCs, and to support modes 1, 2, 3/A, C and 4. The interrogators shall furthermore operate within the simulated target ranges, derived from the summary presented in Section 3.6.1, and in compliance with the user requirements as itemised in Section 2.1.9. These emulated interrogators shall further be compliant with STANAG-4193 [2] timing requirements.

3.6.3.2 Garbled Replies Allowance

Garbled reply situations can be created by situating targets in the same, or close, simulated range from the interrogator being tested.

Requirement:

The system shall allow for the variable programming of emulated target ranges, which are derived from the summary set out in Section 3.6.2.

3.7 Interrogator Concept Summary and Requirements

The subsections below summarise the concept of the digital timing characteristics that are relevant to SSR/IFF interrogators; thereafter, the requirements in respect of the emulated IFF interrogators are allocated. The emulation of interrogators is necessary to satisfy the abovementioned FRUIT and garbled reply requirements.

3.7.1 SSR/IFF Interrogator Concept Summary

The following subsections analyse the operational, timing and functional characteristics related to SSR/IFF interrogators.

3.7.1.1 SSR/IFF Interrogator Operation

In an SSR/IFF system, the interrogator is typically coupled with a primary radar, and it is used to identify targets by generating interrogations to the TxPs attached to those targets. To generate secure mode 4 challenges, an ICC must be connected to the interrogator.

Interrogator reply processing falls outside the scope of this study, as the main aim of this project is to provide SSR/IFF replies to an interrogator signal processor that is being tested.

The concept summaries in Sections 3.4.1.1 and 3.4.1.2 above, including the tables and diagrams, as well as Section 3.4.1.3 in respect of the TxP are also applicable to the emulated interrogator. In situations where the TxP is required to validate the timing of received interrogations, the emulated interrogator must also adhere to the same timing requirements when generating interrogations. It should be noted that the actual processing of secure mode 4 replies and the determination of the target friendliness confidence level form part of the interrogator signal processing tasks and consequently also fall outside the scope of this project (recall Figure 1.1 in respect of the top level project scope).

3.7.2 SSR/IFF Interrogator Requirements

The following subsections present the requirements allocation for the emulated SSR/IFF interrogator.

3.7.2.1 Interrogation Modes

Requirement:

The interrogator shall be able to generate SSR/IFF interrogations in modes 1, 2, 3/A, C and in secure mode 4 if an emulated ICC is connected thereto. This complies with the user requirement set out in Section 2.1.9.

3.7.2.2 Interaction with an ICC

The emulated interrogators must be able to request challenges from the ICC, in order to send them out to the emulated TxPs and TCCs to create FRUIT mode 4 replies.

Requirement:

The interrogator shall be able to request encrypted IFF challenges from the ICC by generating Pre-Trigger (PT) signals whose timing characteristics are compatible with the ICC requirements as discussed in Section 3.8.2.3 below.

3.7.2.3 Interrogation Repetition Rate

STANAG-4193 [2] limits the maximum number of interrogations an interrogator can generate per second, and it recommends operation at the lowest practical rate. The purpose of this is most likely to help minimize the amount of challenges and replies in space, and to allow TxP and interrogator signal processors to perform their housekeeping tasks between interrogations/replies.

Requirement:

In compliance with paragraph 3.2.5 in STANAG-419 [2], the interrogator shall not generate more than 450 interrogations per second for all SSR/IFF modes.

3.8 ICC Concept Summary and Requirements

The main purpose of the SSR/IFF target emulator is to provide replies to an interrogator being tested; however, the emulator must also be able to create effects caused by other interrogators operating in the area. Recalling Figure 3.1, the emulation of IFF ICCs is necessary in order to emulate secure mode 4 challenges. This is needed to cause FRUIT and garbled mode 4 replies. The subsections below present an ICC relevant concept summary of cryptographic and digital timing characteristics, followed by a listing of the requirements in respect of the emulated ICC.

3.8.1 IFF ICC Concept Summary

To meet relevant aspects of the user requirements, the following subsection analyses the related IFF ICC operational and functional characteristics and timing requirements, which the system must adhere to in accordance with STANAG-4193, especially Appendix 3 of Annex A [2].

3.8.1.1 ICC-Interrogator Operation Sequence

Figure 3.13 below depicts the signalling sequence and timing of a secure mode 4 challenge request made by the interrogator to the ICC, followed by the generation of the challenge, and the reply delay to be expected by the interrogator if a successful decryption of the challenge is completed by the TCC.

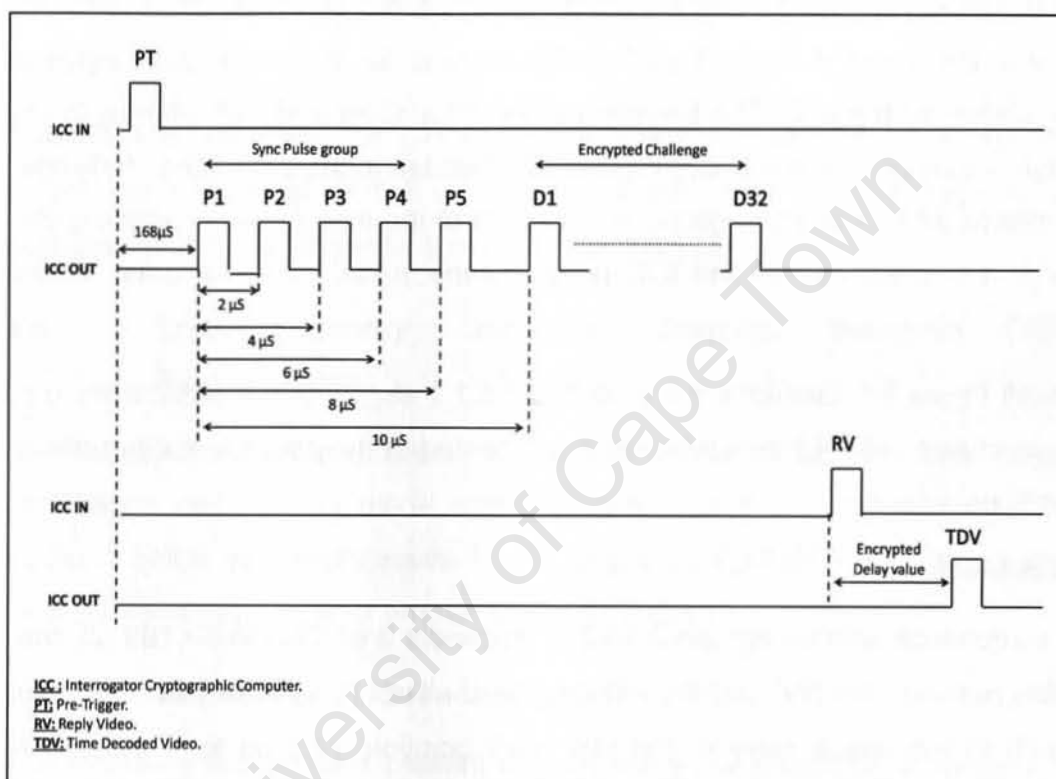


Figure 3.13 : IFF secure mode 4 interrogator to ICC interaction. The interrogator requests an encrypted challenge from the ICC by sending a Pre-Trigger (PT) pulse; the ICC responds with the sync pulse group and the encrypted challenge. For the interrogator to be aware of when to expect the reply from a friendly TxP, it needs to know the delay value encrypted in the challenge as described in Figure 3.6, and for that, it queries the ICC by sending the Reply Video (RV) pulse. The delay measured until the ICC generates the Time Decoded Video (TDV) pulse is equivalent to the encrypted delay.

3.8.2 IFF ICC Requirements

The following subsections present the requirements in respect of the emulated IFF ICC.

3.8.2.1 ICC Processing Rate

Requirement:

The ICC shall be able to accept a maximum of 1800 Pre-Triggers (or challenge requests) per second. This is in compliance with paragraph 2.5.1 of Appendix 3 of STANAG-4193 [2].

3.8.2.2 Reply Video to Time Decoded Video Encrypted Delay

As depicted in Figure 3.6 and Figure 3.13, the interrogator must know when to expect the mode 4 reply from friendly aircrafts for a specific interrogation generated by the ICC. The interrogator will thus send a signal referred to as Reply Video (RV) to the ICC. The delay embedded in the encrypted challenge is measured by the interrogator, which refers to the time between sending the RV to the instant when the ICC produces the signal Time Decoded Video (TDV).

Recall Figure 3.8, Sections 3.4.2.10 and 3.5.1.1 above, which summarise the concept and set out the requirements connected to the possible sixteen delay positions.

Requirement:

In compliance with paragraph 2.10.2 of Appendix 3 of STANAG-4193 [2], the delay between the RV and the TDV signal shall not be greater than 2.5 μ s in which to indicate a reply in the last reply position, and up to a maximum duration of 60 μ s for a reply in the first reply position.

3.8.2.3 Pre-Trigger (PT) Pulse Width Validation

Requirement:

The ICC shall validate the pulse width of the received Pre-Trigger pulse, and accept pulses with a minimum duration of 0.5 μ s and a maximum duration of 10.0 μ s, in compliance with the relevant aspects of paragraph 2.5.1 of Appendix 3 of STANAG-4193 [2].

3.8.2.4 Reply Video (RV) Pulse Width Validation

Requirement:

The ICC shall validate the pulse width of the received RV pulse and accept pulses with a minimum duration of 0.4 μ S and a maximum duration of 0.6 μ S, in compliance with relevant aspects of paragraph 2.9 of Appendix 3 of STANAG-4193 [2].

3.8.2.5 Time Decoded Video (TDV) Pulse Interval

Requirement:

The ICC shall generate the TDV pulse with a minimum duration of 0.3 μ S and a maximum duration of 0.7 μ S, in compliance with relevant aspects of paragraph 2.10.1 of Appendix 3 of STANAG-4193 [2].

3.9 Target Identity Generator Concept Summary and Requirements

In order for the system to create and maintain distinct targets, some target parameters need to be made available to the user for configuration. The sections below list requirements for the target configuration parameters and for the minimum number of emulated targets required.

3.9.1 Target Identity Generator Requirements

The following subsections present the requirements allocation in respect of the target identity generator.

3.9.1.1 Target Configuration Parameters

Requirements:

In order for the system user to create an SSR/IFF target, the following target parameters shall be configurable and maintained by the system once configured:

- a) Target range (from the interrogator being tested).
- b) Target range change rate, i.e. the speed of the approaching target or of the target travelling away from the interrogator being tested.

- c) Target azimuth, i.e. the range of ACP pulses in which the target is illuminated.
- d) Target azimuth change rate, i.e. the azimuth change for the next antenna rotation.
- e) Target TxP-TCC pair A, B, C and D codes as described in Table 3.11, M4 key, interrogation modes enable/disable control, SPI and emergency enable/disable control.

3.9.1.2 Number of Targets

Requirement:

The system shall be able to emulate and maintain from 0 to at least 1,500 targets in a single antenna sweep; these targets may be evenly distributed in a 360° space.

3.10 Target Mobility Manager Concept Summary and Requirements

In order for the SSR/IFF emulator to provide emulated targets in motion that reply to interrogations from the interrogator being tested, or from the FRUIT interrogators discussed in Section 3.6, it is necessary to understand target mobility in both range and azimuth from the SSR/IFF perspective, in order to specify what the system should do or what must be available to the user for configuration. The subsections below present a target mobility concept summary and a list of the requirements derived from this concept summary.

3.10.1 Target Mobility Manager Concept Summary

The subsections below analyse the following:

- Antenna interface ACP/ARP pulses
- The relation between target range and interrogator PRF
- Target illumination time and ACP count relation
- Target angular velocity and ACP count relation.

The aim by looking at these topics is to explain how targets will change in azimuth and range, and how this will need to be incorporated in the system design.

3.10.1.1 Antenna Interface ACP/ARP Pulses

The SSR/IFF antenna will provide azimuth information for 360° by generating a train of pulses known as Azimuth Change Pulses (ACP), which consist of 4096 pulses in the case of the antenna provided by the user. The pulse count determines the angle of the antenna with a precision obtained by dividing 360° by the number of ACP pulses. The Azimuth Reference Pulse (ARP) is a reset pulse, which indicates a new count of ACP pulses, which in turn indicates a new antenna rotation.

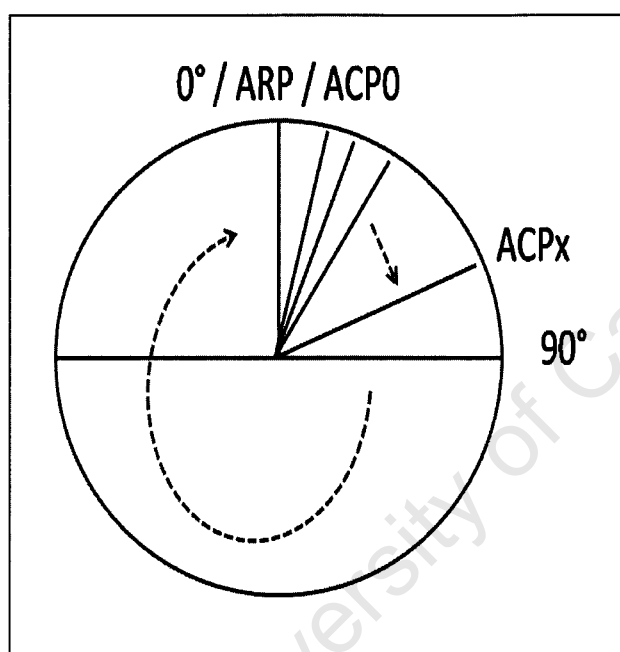


Figure 3.14 : The ACP pulse count represents the azimuth of the antenna, where the azimuth increases with every ACP pulse in a precision obtained by dividing the 360° over the fixed number of pulses. The ARP pulse is used to reset the ACP pulses count and occurs at the beginning of each new antenna rotation.

The interrogator processor being tested will use the ACP count provided by the antenna as a means of determining the target bearing. The spacing between ACP counts is dependent on the antenna rotation period as follows:

$$ACP \text{ spacing} = \frac{\text{Antenna Rotation Period}}{ACP \text{ Counts per rotation}} \quad (3.2)$$

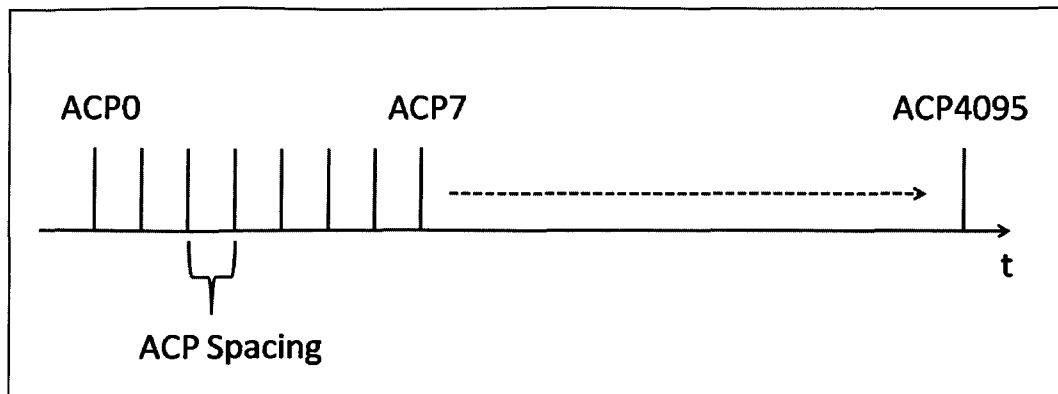


Figure 3.15 : ACP spacing is the time between two ACP pulses

The system must interface with or simulate an antenna with a rotation period of 8 seconds and an ACP count of 4096, therefore:

$$ACP\ Spacing = \frac{8s}{4096} = 1.95\ ms \quad (3.3)$$

During a certain ACP count, the interrogator will assume that any received replies are from targets at the same fixed azimuth until the next ACP count is received, whereafter the azimuth is increased, and so on.

3.10.1.2 Target Range and Interrogator PRF

The system is required to emulate targets from 0 to 600 km in range. In order for an interrogator to detect targets at such a distance of 600km, a PRI of at least 4 ms is required, and a 3 μs TxP processing time is added for SIF modes and 202 μs in mode 4. This PRI is required to accommodate the two-way trip of the challenge/reply operation. An example of a calculation for SIF modes using Equation 3.1 shows that the time interval between interrogations would be:

$$PRI = \frac{600Km}{c} * 2 + TxP\ Delay = 4.003\ ms \quad (3.4)$$

Where C is the speed of light. This PRI will force the interrogator to have a PRF of at least 250 Hz.

3.10.1.3 Target Illumination Time and ACP Count Relation

The system must interface with or simulate an antenna with an EBW of 5° and a rotation period of 8 seconds. In terms of Section 3.10.1.2 above, the PRF of the interrogator is 250 Hz, and it has an EBW of 5° (a 360° space can be divided into 72 sectors of 5° each). The target illumination time for an assumed stationary target with an antenna rotation time of 8 seconds will be:

$$\text{Target Illumination Time} = \frac{8s}{72} = 111 \text{ ms} \quad (3.5)$$

While a target is located in the EBW, it can be interrogated with a number of interrogations, calculated as follows:

$$\text{Number of Interrogations in EBW} = \text{PRF} * \text{Target Illumination Time} \quad (3.6)$$

$$\text{Number of Interrogations in EBW} = 250 * 111\text{ms} = 28 \text{ Interrogations} \quad (3.7)$$

The ACP pulses count from the antenna in 8 seconds is 4096, which equates to 512 pulses per second; therefore, the number of ACP pulse changes during the illumination time is calculated as follows:

$$\text{ACP Pulses During Illumination} = 111 \text{ ms} * 512 = 56.32 \text{ pulses} \quad (3.8)$$

Based on the above, it is clear that the emulator needs to make targets available based on the current ACP pulse count provided by the antenna or generated internally. The validity of targets during certain ACP pulse counts needs to be configurable, in order to interface with or simulate antennas with different EBWs and rotation periods. Figure 3.16 presents a graphical representation of the above.

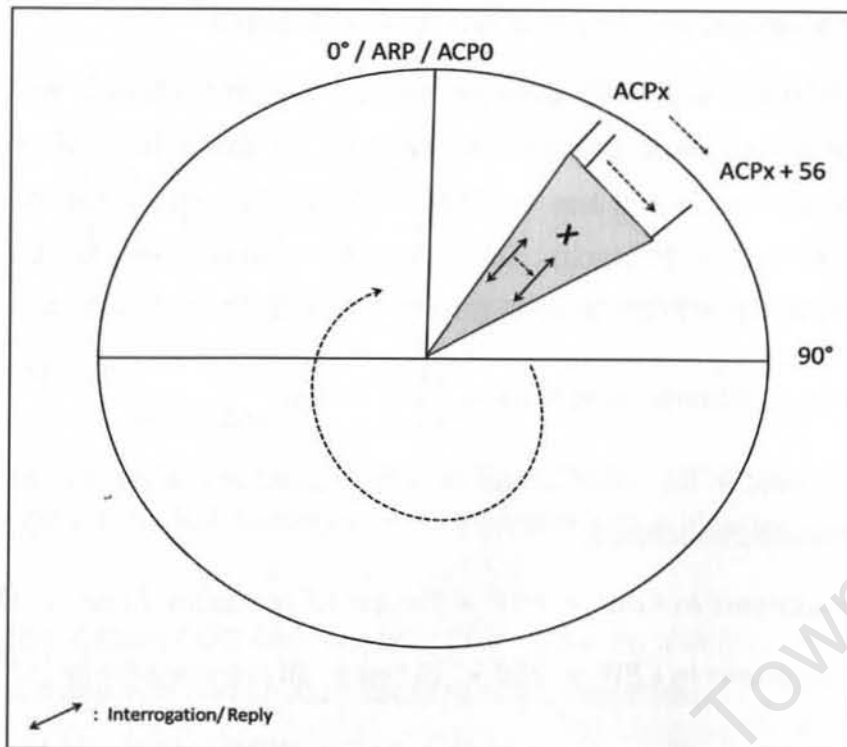


Figure 3.16 : The emulated target labelled "X" is assumed to be stationary and to be located in the illumination area of the 5° EBW antenna, which is rotating once every 8 seconds, thus resulting in an illumination time of 111ms. The target will be illuminated for approximately 56 ACP pulses, based on a 4096 ACP pulse count antenna. The target will receive approximately 28 interrogations while illuminated.

3.10.1.4 Target Angular Velocity and ACP Count Relation

In the next antenna rotation, after being detected in the first, the azimuth range of a target travelling in a circle around the interrogator will depend on the target's angular velocity and range, as seen in the target illumination summary in Section 3.10.1.3 above and Figure 3.16. The azimuth will change at a lower rate for a target at a further range from the interrogator than for a target that is at a closer range. Angular velocity w is defined as:

$$w = \frac{v}{r} \quad (3.9)$$

Where v is the linear velocity and r is the radius. For a target travelling at 200 m/s and at a range of 600 km, the angular velocity is:

$$w = \frac{200\text{m/s}}{600\text{Km}} = 3.33e^{-4} \text{ rad/s} \quad (3.10)$$

To calculate the azimuth change in degrees, the result is multiplied by $\frac{180}{\pi}$ to obtain a result of 0.019°/s. For an antenna providing 4096 ACP pulses for 360°, an ACP pulse equivalence in degrees is calculated by dividing 360° by 4096, thus resulting in 0.087°. For an antenna rotating once every 8 seconds, the azimuth change in degrees will be calculated by multiplying 0.019°/s by 8, resulting in a change of 0.152° in 8 seconds. The azimuth change rate in ACP is what will finally be used by the emulator; it is calculated by dividing the azimuth change in 8 seconds by the azimuth change in one ACP as follows:

$$\text{Change in ACPs} = \frac{0.152}{0.087} = 1.74 \text{ ACPs} \quad (3.11)$$

In accordance with the above example, the emulator must move the target ACP range by around 2 ACP pulses for every new antenna rotation, as illustrated in Figure 3.17 below.

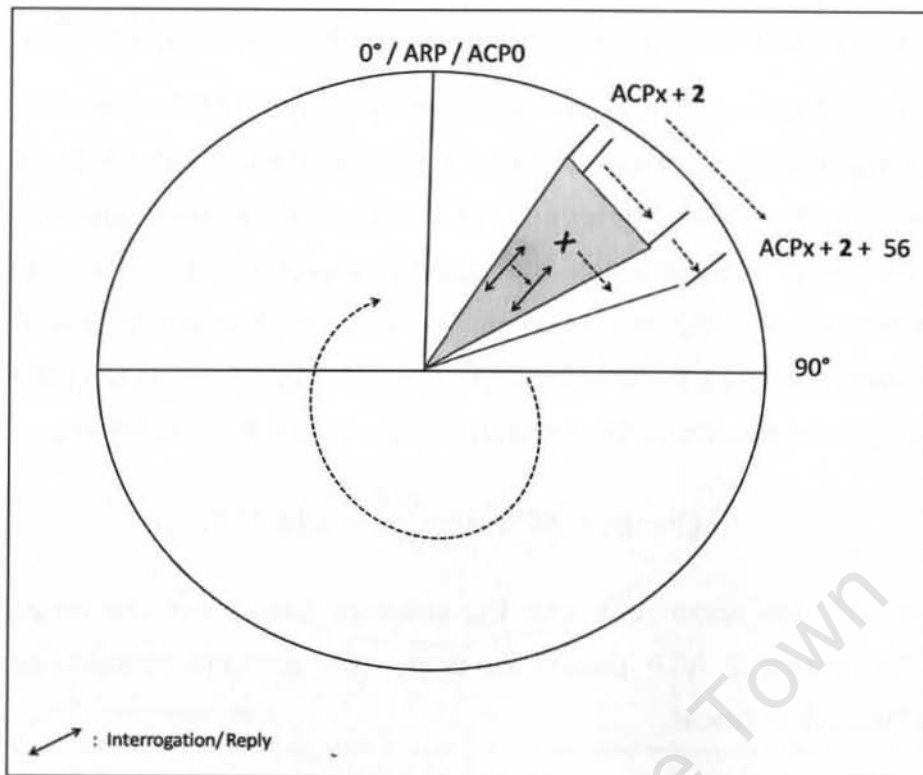


Figure 3.17 : Recalling Figure 3.16, the emulated target labelled "X" is travelling in a uniform circle and is at a range of 600km from the interrogator with an angular velocity of $3.33e^{-4} \text{ rad/s}$, based on Equation 4.9. The target will change in azimuth by 0.152° for the next antenna rotation in 8 seconds, resulting in a shift in the ACP pulses range by approximately 2, based on Equation 4.10.

3.10.2 Target Mobility Manager Requirements

The following subsections present the requirements allocation in respect of the target mobility manager.

3.10.2.1 Antenna ACP/ARP Interface and Simulation

Requirements:

The system shall be able to:

- Accept TTL ACP/ARP pulses from an SSR/IFF antenna providing 4096 ACP counts per rotation.
- Generate the ACP/ARP pulses in the absence of the abovementioned antenna.
- Make the azimuth range of emulated targets configurable for the simulation of different target behaviour, range and speed.

3.10.2.2 Antenna Variation

Requirement:

The system shall be able to interface with antennas with different rotation periods, ACP pulse counts and EBWs. More specifically, however, the system must demonstrate its capability for a 5° EBW antenna.

3.11 Continuous Operation Manager Concept Summary and Requirements

The user requires the system to operate in a continuous live mode. In this mode, interrogation/reply parameters must be able to change on-the-fly without it being necessary to restart the system. The system must furthermore ensure that the system user has live access to the emulated targets, interrogators, TxPs and TCCs.

3.11.1 Continuous Operation Manager Requirements

The subsection below presents the requirements allocation in respect of the continuous operation manager.

3.11.1.1 Target Range and Existence

Requirements:

The system shall allow the following:

- a) Emulated targets shall be allowed to travel towards the interrogator being tested, i.e. the reply delay will decrease as the emulated target comes closer to the interrogator until the minimum simulated range, before it travels away until the maximum range, and so on, to allow for continuous operation regardless of the duration of the test.
- b) Emulated FRUIT interrogator parameters shall be allowed to change during a test without it being necessary to restart the test. This is also applicable to the emulated TxPs and TCCs.

3.12 Real-Time Operation Manager Concept Summary and Requirements

The target emulator system is required to operate in real time, in the sense that replies from emulated targets in response to interrogations from the interrogator being tested, or from emulated FRUIT interrogators, must always be proportional to the emulated target's range and the target's angular velocity. Furthermore, the timing requirements must be in accordance with STANAG-4193 [2] for TxP-TCC processing times.

Aspects contributing to the ability of the system to operate in real time are discussed in all the above-mentioned project subsystem concept summaries covered in this chapter. The real-time requirement will thus automatically be satisfied when all the timing requirements are satisfied for all the subsystems.

3.13 ITRC Interface Requirements

The ITRC is an RF SSR/IFF test transceiver card that is currently being developed by another Masters student in the RRSg at UCT; it is being designed to provide an RF level input/output interface to the interrogator being tested. The ITRC should be able to interface with SSR/IFF related laboratory equipment, including the SSR/IFF target emulator. The SSR/IFF emulator design is required to create an interface point for the ITRC.

Requirement:

The system shall provide an interface point for the ITRC, which will allow it to use the target emulator as a digital back-end.

3.14 HW Interface Requirements

Input/output TTL pins are available on the target HW board, and should be used as the interface with the interrogator being tested.

Requirements:

The SSR/IFF target emulator shall make the following signals available for testing and integration purposes:

Table 3.14 : SSR/IFF emulator input/output signals

Signal	Description	Direction
ACP Pulses	ACPs received from an SSR/IFF antenna or generated by the system	input/output
ARP Pulses	ARPs received from an SSR/IFF antenna or generated by the system	input/output
DSP External Memory Interface A External Memory Interface (EMIF-A) clock	EMIF- A clock may be used to synchronize several parts of the system, which will be covered in the design chapter	output
Combined interrogations	Interrogations received from the interrogator being tested combined with FRUIT interrogations generated by the system	input/output
ACP count	12 lines to represent 4096 ACP count	output
Combined Replies	Combined replies generated by all emulated targets	output

3.15 User Requirements Traceability Matrix

Table 7.1 in Appendix A represents a traceability matrix, which maps the user requirements itemised and discussed in Chapter 2 against the requirements set out in this chapter. One of the benefits of this mapping is that it proves that all the user requirements have been covered, thereby ensuring that every user requirement has been analysed and that further requirements have been derived and allocated to satisfy them.

3.16 Summary

The above chapter began by presenting a system block diagram of the SSR/IFF emulator, based on an analysis of the user requirements contained in the preceding chapter. For each subsystem in this diagram, a concept summary was presented and requirements were allocated. A link to the user requirements traceability matrix was provided at the end of the chapter. The

following chapter will present the detailed design of the system and the tradeoffs that were necessary in order to implement it.

University of Cape Town

4. Chapter 4: System Design

The following chapter presents the design of the SSR/IFF emulator. The two main computers on the target HW provided by the user are an FPGA and a DSP. The computers are presented in a target HW overview section, which is followed by a top-level concept design summary. Certain parts of the design are partitioned over the DSP or the FPGA. The tradeoffs and reasoning behind the partitioning will also be presented. A detailed design of the FPGA and DSP parts of the system will be covered in depth later in the chapter.

4.1 Target HW Overview

The Quixote board [8] shown in Figure 2.1 contains two main computers, a Texas Instruments TMS320C6416 DSP and a six-million-gate Xilinx XC2V6000 VirtexII FPGA. On-board memories available are a 32 MB SDRAM and an 8 MB ZBT SBSRAM.

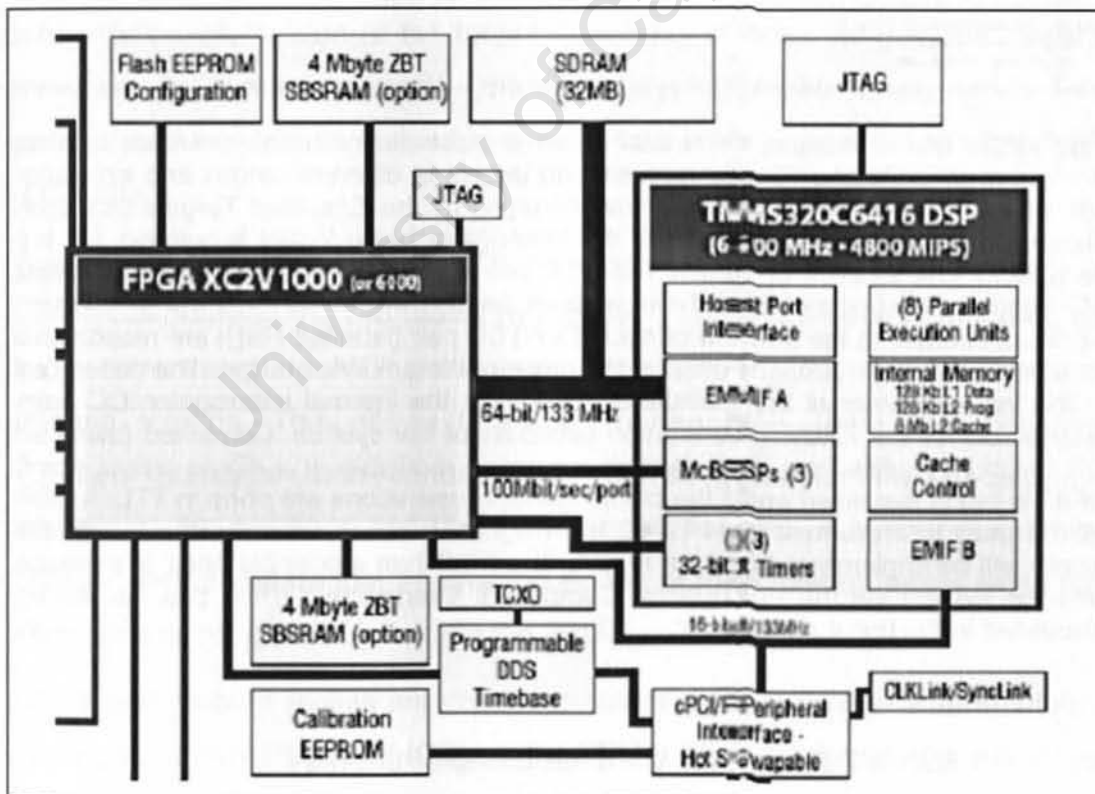


Figure 4.1 : From [14]. The two main computers on the Quixote board are the Xilinx XC2V6000 VirtexII FPGA and the Texas Instruments (TI) TMS320C6416 DSP.

4.2 SSR/IFF Emulator Top-Level Block Diagram

Figure 4.2 illustrates a top-level diagram of the system.

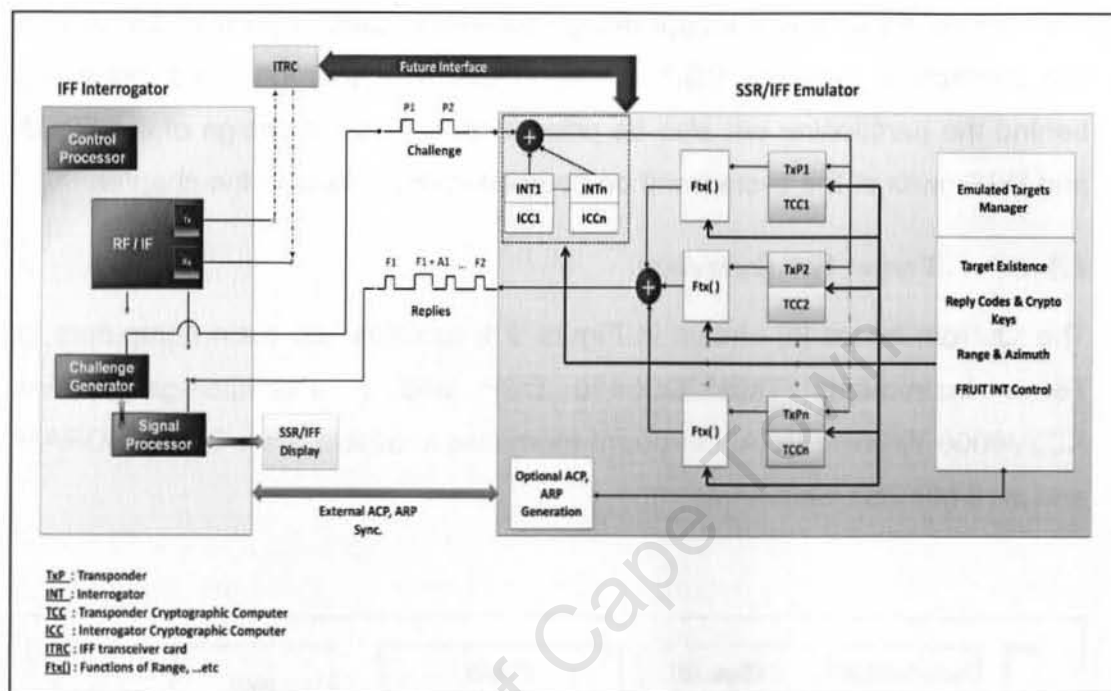


Figure 4.2 : SSR/IFF target emulator top-level block diagram. The emulator consists of a group of TxPs and TCCs representing targets at different ranges and azimuths, with different reply codes. Targets are managed by the Emulated Targets Manager, depending on where the antenna of the interrogator being tested is pointing, i.e. the personality and location of each Txp-TCC pair changes, depending on the current ACP count. See description of concepts in Section 4.3 below. The range function blocks connected to the output of each TxP-TCC pair (labelled Ftx()) are responsible for delaying the reply, depending on the range of the emulated target. The dotted box in the top left corner of the emulator represents the internal interrogator-ICC pairs responsible for the FRUIT generation capability of the system. Combined (using an OR function) replies from the system are made available at a single output point. RF/IF is being bypassed and the challenge/reply operations are done in TTL. A DSP will be used to implement the Emulated Targets Manager, whereas the rest of the blocks will be implemented on an FPGA. The ITRC has a possible point of interface with the system via the Peripheral Component Interconnect (PCI) bus, as will be discussed in Section 4.4.2 below.

4.3 SSR/IFF Emulator Concept Design Summary

The design concept exploits the relatively slow timing characteristics of SSR/IFF systems, where antenna rotations are measured in seconds, and

interrogation repetition rates are capped by STANAG4193 [2] and are typically measured in milliseconds. This allows sufficient computing time for a DSP running on a 1 GHz clock, and an FPGA running on a 100 MHz clock. The design is based on using only eight TxP-TCC pairs, which reside in the FPGA, to emulate thousands of targets, exceeding the 1500 targets required by the user. The eight TxP-TCC pairs are divided into two groups each comprising four pairs, between which received interrogations will ping-pong. TxP-TCC pairs in the FPGA are fully configurable and are made available as asynchronous memory interfaced to the DSP. On the DSP, the registers of the TXP-TCC pairs are recognised as asynchronous memory and are defined in such a way that they are available for TxP-TCC configuration by the SW running on the DSP.

The personalities of the TxP-TCC pairs are updated by the DSP, based on interrupts from the FPGA when an ACP/ARP pulse is detected. After an ACP count is read by the DSP, it is used to access a look-up table, managed by the DSP, which resides in the SDRAM, and contains the relevant configuration information of the targets (i.e. reply codes, ranges, the target's presence in current azimuth, mode 4 cryptography keys, etc.) This configuration information is used to update the personalities of the eight TxP-TCC pairs.

The look-up table in the SDRAM is mirrored, and a ping-pong operation is carried out between the two tables by the DSP. This operation is triggered by the occurrence of an ARP pulse interrupt indicating the completion of an antenna rotation. This allows the DSP to use the spare time between ACP/ARP interrupts (milliseconds for ACP and seconds for ARP) to calculate changes in the positions and ranges of targets for the subsequent antenna rotation, and to update that information in one of the look-up tables while the other table is being used to update the FPGA.

FRUIT and garbled replies are created by placing four configurable emulated interrogator transmitters and ICCs on the FPGA. The DSP is able to select the FRUIT interrogator's interrogation modes and PRFs.

In order for replies from the targets to be delayed based on their range, TxPs use First In First Out (FIFO) memories in the FPGA to store their generated reply for a specified period of time. This time period is calculated based on the target's range, the duration of the two-way interrogation/reply and the TxP processing time. The following subsections will expand on the aspects discussed in the above summary.

4.4 Design Partitioning Decisions

The subsections below describe the partitioning of the design units, which enables them to run on the two major computing engines on the board. The relevant choices regarding partitioning are explained and justified where needed.

4.4.1 FPGA Partition

According to the timing requirements for TxPs, CCs and interrogators presented in Chapter 3, SSR/IFF pulse widths and durations need to comply with timing within a range of between 450 ns to 800 ns, and they must be able to detect tolerance margins as low as 50 ns. The multi target system requirement was the reason behind the design decision to place multi target instances in the VirtexII FPGA, as it is suitable for handling a minimum clock speed of 40 MHz (which is required to detect a 50 ns transition) and multiple instances of functional blocks in parallel. Interfacing with the antenna of the interrogator being tested via the ACP/ARP signals is also handled by the FPGA, which allows dedicated circuitry to monitor the ACP/ARP lines and to emulate their presence if an antenna is not provided by the user.

Due to the system's target range requirement, replies from targets must be delayed before being sent out to the interrogator being tested. FIFOs on the FPGA have thus been chosen to store the replies until they are sent out, since the XC2V6000 VirtexII device is considered memory rich with a maximum RAM of 2,592 Kbits [13].

4.4.2 DSP Partition

The multiple distinct identity targets, target mobility and system continuous operation requirements are management and control orientated, which

necessitates intensive calculations to be made continuously in order to update target locations and identities. This is suitable for the TI TMS320C6416 DSP, as it runs on a 1 GHz clock. The decision to allocate target management functions to the DSP has been influenced by the relative simplicity of C code programming and the enhanced debugging capabilities on the DSP in Code Composer Studio (CCS). CCS is the Integrated Development Environment (IDE) from TI. The possible inclusion of an interface with a host PC over the PCI bus as a future expansion of this project is an additional motivation for placing target management functions on the DSP. A future expansion may include the development of a sophisticated PC application with a Graphical User Interface (GUI) in order to create mobile target scenarios and to allow the information to be sent from the PC to the DSP, which is available on the PCI bus. The outputs of the interrogator processor may then be compared with the mobile target scenarios, in order to create a more advanced interrogator testing capability. The availability of the DSP on the PCI bus also allows for a possible interface point for the ITRC.

4.5 SSR/IFF Target Emulator FPGA Detailed Design

Figure 4.4 presents the FPGA design for the system. Data is exchanged between the FPGA and the DSP via an asynchronous memory interface, which utilises 128 read/write registers. These registers are used by the DSP to configure and change the personalities and locations of the eight TxP-CC pairs, to configure the FRUIT interrogators for the interrogation modes and PRFs, and to enable/disable and acknowledge interrupts. Registers read by the DSP are also used to check an interrupt cause, as in Table 4.2, and to read the current antenna position indicated by the ACP count, as in Table 4.1. The registers are defined in Table 4.8.

The DSP asynchronous memory interface clock is provided to the FPGA, and it is used to clock the design. The antenna position interface and emulation block is responsible for interfacing with an SSR/IFF antenna, or emulating it by supplying ACP/ARP pulses to the rest of the system and the current ACP count to the DSP.

Table 4.1: Antenna ACP Count (ACPC) register bits allocation

31	12	11	...	0
Reserved			ACP Count 0 – 4095		

The interrupts controller block accepts interrupt requests from the antenna interface block and multiplexes the interrupt requests to one line connected to the DSP external interrupt pin. This design provides the DSP with a register to write to that either allows or masks specific interrupt types from causing an interrupt request. A register to clear interrupts is used by the DSP to acknowledge an interrupt after reading an interrupt pending register, which indicates the cause of the interrupt. Once all interrupts have been acknowledged, the interrupts controller deactivates the interrupt line to the DSP.

Table 4.2: Interrupt Pending Register (IPR) bits allocation

7	6	5	4	3	2	1	0
Reserved						ARP Interrupt	ACP Increment Interrupt
15	14	13	12	11	10	9	8
Reserved							
23	22	21	20	19	18	17	16
Reserved							
31	30	29	28	27	26	25	24
Reserved							

Eight TxP-TCC pairs (divided into two groups) are used to receive interrogations in a ping-pong manner toggled by ACP pulses. The ping-pong architecture is used to satisfy the system requirement for maximum target range, and will ensure that the TxP-TCC pair, which is busy processing an interrogation and delaying the reply (depending on the target range) is allowed a twice the time delay between two ACP pulses before it is requested to process another interrogation. During such time, the group not processing interrogations becomes available after the occurrence of the second ACP pulse. See Figure 4.3 below for an illustration of this.

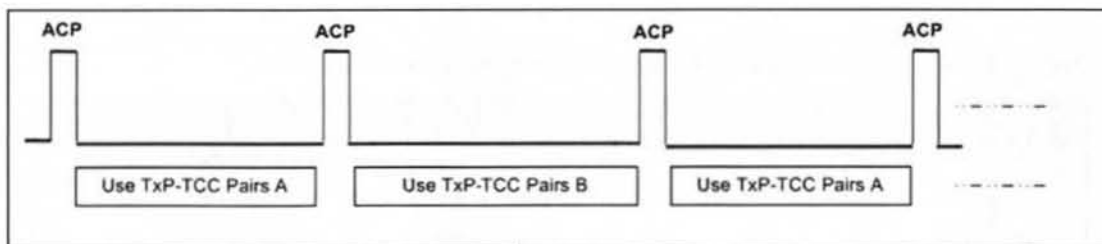


Figure 4.3 : Eight TxP-TCC pairs are divided into two groups, A and B. They are used to receive interrogations in a ping-pong manner, toggled by ACP pulses.

The DSP application is unaware of the mirroring, and assumes the existence of only four TxP-TCC pairs, according to which the configuration registers connected to the first four pairs are also connected to the second four in the same manner. For the antenna with an 8 s rotation period and 4096 ACPs/s (specified by the user), the duration of time between ACPs is around 1.95 ms, as shown in Equation 3.3, and 3.9 ms between any three ACPs. This allows the system to emulate replies from targets at a maximum range of around 600km, taking the two-way challenge/reply trip time into account.

Interrogations from the four FRUIT interrogators are combined with the interrogations from the interrogator being tested, and are thereafter routed to the TxP-TCC groups. FRUIT interrogators are similarly configured to the TxP-TCC by the provision of a register to the DSP in order to allow it to enable/disable an interrogator, and to select the interrogation mode and PRF, as in Table 4.3.

Table 4.3: Interrogator(x) Information Register (IIRx) bits allocation

7	6	5	4	3	2	1	0
Reserved			Enable/Disable (1/0)	Interrogation Mode :			
				0000 : N/A			
				0001 : Mode 1			
				0010 : Mode 2			
				0011: Mode 3/A			
				0100 : Secure Mode 4			
				0101: Mode C			
15	14	13	12	11	10	9	8
PRI in steps of 10ns							
23	22	21	20	19	18	17	16
PRI in steps of 10ns							
31	30	29	28	27	26	25	24
PRI in steps of 10ns							

The system combined replies are made available as an output to the interrogator being tested.

4.5.1 TxP and TCC Design

The sections below discuss the TxP-TCC design and interface.

4.5.1.1 TxP-TCC Block Diagram

In order to meet the re-configurability requirements of the TxP-TCC, the TxP-TCC in Figure 4.5 is designed to be generic, which means that it is able to accept all input configuration parameters from asynchronous memory interfaced registers, namely:

- The A, B, C, and D reply codes (recall Table 3.10)
- The mode 4 decryption key (the usage of this key is illustrated in Figure 4.6)
- Video input in respect of received interrogations from the interrogator being tested or from the FRUIT interrogators
- Enable/Disable status for SIF/Mode 4 and SPI/Emergency replies
- A delay value input corresponding to the range of the emulated target carrying the TxP-TCC pair
- Clock and reset ports for synchronization and initialization of the design

The SIF or mode 4 reply, a mode 4 disparity (which indicates the failure of a mode 4 challenge decryption) and the TxP busy signal are made available as outputs. The disparity, probe and busy signals are unused during operation and are only for debugging purposes.

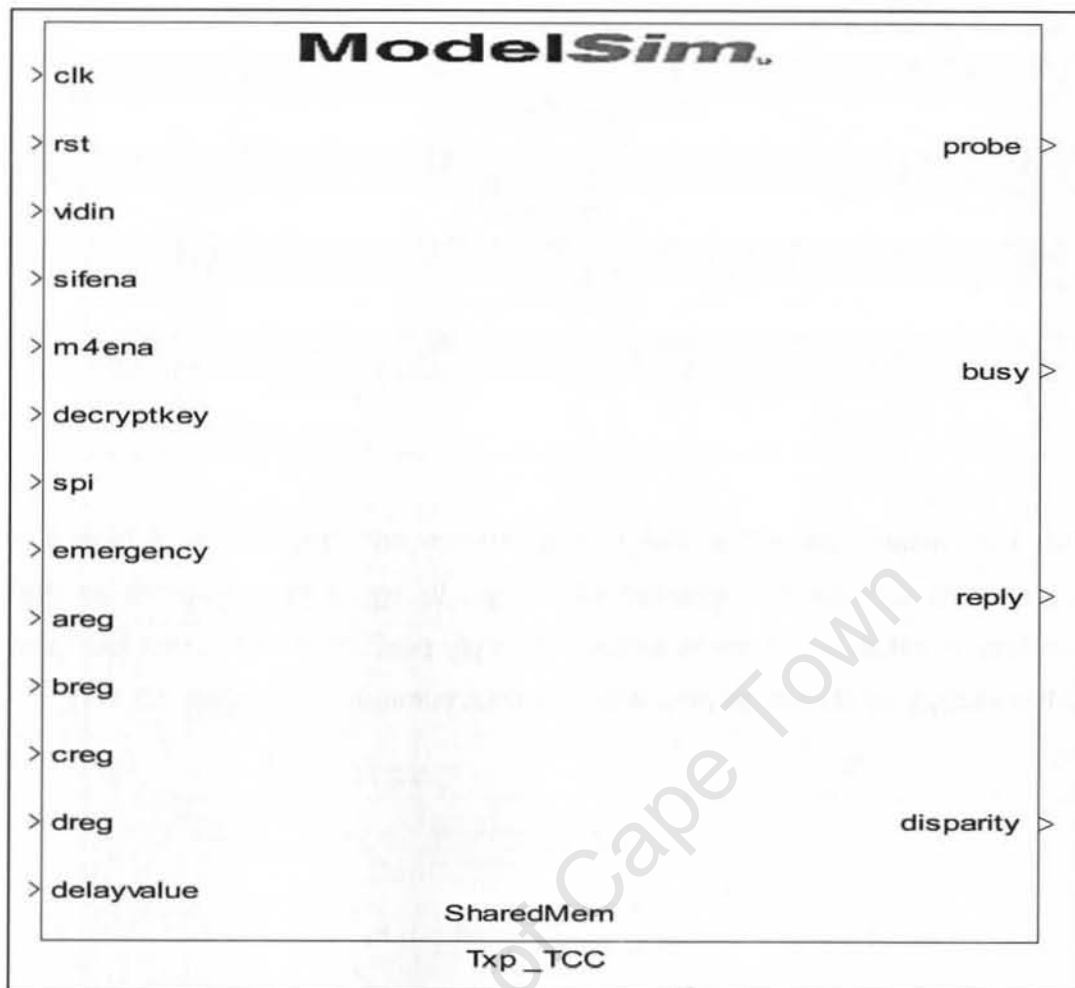


Figure 4.5 : TxP-TCC block diagram showing the inputs and outputs

4.5.1.2 TxP-TCC Interrogation Detection and Reply Generation Process

The algorithm followed for the detection of SIF or secure mode interrogations and to generate the replies is presented in Figure 4.6. Table 4.4 contains the bits definition of the clear-text secure mode 4 challenge selected by the author as a basic encryption scheme, and a place holder for future custom cryptography enhancements.

Table 4.4: Plain-text M4 challenge definition

7	6	5	4	3	2	1	0
Verification Byte = 0x5A							
15	14	13	12	11	10	9	8
Reserved							
23	22	21	20	19	18	17	16
Reserved							
31	30	29	28	27	26	25	24
Secure Reply Position (M4 Reply Delay)				Reserved			

The TCC makes use of the DSP configurable mode 4 key shown in Table 4.7 in order to decrypt the received challenge, to verify the existence of the verification value, and then to extract the reply position from the last four bits of the decrypted challenge (recall the concept summary in Section 3.5.1.1).

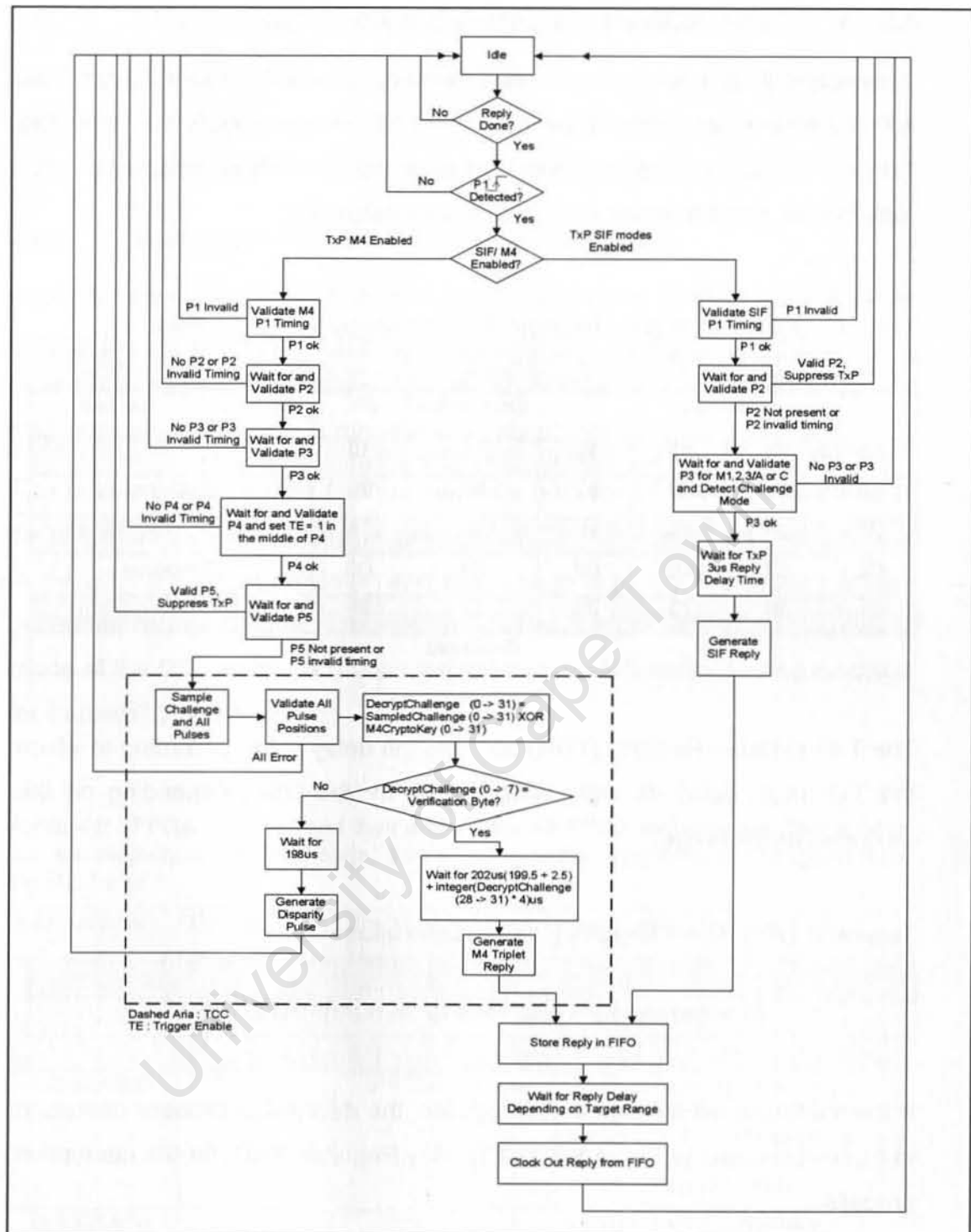


Figure 4.6 : TxP and TCC interrogation detection and reply process. The TxP-TCC pair is to be implemented in VHDL on the VirtexII FPGA. P2 and P5 tests are for sidelobe suppression for SIF and secure mode respectively. The cryptography operation shown in the TCC, which is an exclusive or (XOR) of a key with the received challenge to extract the clear-text challenge, is specific to the SSR/IFF target emulator and it was chosen for demonstration only. It can be considered as a place holder for future cryptography development.

4.5.1.3 TxP-TCC Register Interface Bits Allocation

For each TxP, the sets of registers defined in Table 4.5, Table 4.6 and Table 4.7 are created and programmed by the DSP at every ACP interrupt. The TxP(x) Information Register (TIR) is used to set the TxP personality i.e. SIF reply codes, and SIF/mode 4 enable/disable status, etc.

Table 4.5: TxP(x) Information Register (TIR) bits allocation. (1 = enable)

7	6	5	4	3	2	1	0
Reserved				Emergency	SPI	M4Ena	SIFEna
15	14	13	12	11	10	9	8
A2	A1	A0	B2	B1	B0	Reserved	
23	22	21	20	19	18	17	16
C2	C1	C0	D2	D1	D0	Reserved	
31	30	29	28	27	26	25	24
Reserved							

The TxP(x) Delay Register (TDR) contains the delay value according to which the TxP must delay its reply which is set by the DSP, depending on the emulated target range.

Table 4.6: TxP(x) Delay Register (TDR) bits allocation

31	0
32 bit representing a delay value for the reply in steps of 10ns		

If the TxP receives a mode 4 interrogation, the decryption process described in Figure 4.6 uses the key in the TCC(x) Key Register (TKR) for the decryption process.

Table 4.7: TCC(x) Key Register (TKR) bits allocation

31	0
32 bit TCC mode 4 challenge decryption key		

4.6 SSR/IFF Target emulator DSP Detailed Design

The emulated target identity and mobility management and continuous operation requirements are handled by the DSP (recall Figure 3.1). The following sections will expand on major DSP SW design issues.

4.6.1 DSP-FPGA Asynchronous Memory Interface

Figure 4.1 shows that the HW implementation allows the EMIF-A of the DSP to access the VirtexII FPGA. The EMIF-A controller configuration values have been taken from the board user manual [14], and have been verified using the DSP memory map tables in the DSP data sheet [15].

The registers used by the DSP to interface with the FPGA are presented in Table 4.8 along with their usage descriptions. All the registers are proprietary to the SSR/IFF target emulator, and their usage is part of the system design presented in this chapter. The registers fall within the EMIF-A chip-select 0 range of the DSP and their names are used in the SW without being modified for traceability purposes.

Table 4.8 : FPGA registers and their addresses. All FPGA registers are 32 bits wide and the majority are in R/W mode, thus allowing better insight when debugging from the DSP side.

Hex Address	Decimal offset Address in FPGA	Register Name	Type	Description
0x80000000	0	IPRCLR	r/w	Interrupt Pending Clear Register stores acknowledgments from the DSP to the corresponding interrupts in the Interrupt Pending Register (IPR)
0x80020000	2	IPR	r	Interrupt Pending Register stores all the FPGA interrupts
0x80040000	4	IMR	r/w	Interrupt Masking Register values indicates which FPGA interrupts should be enabled
0x80060000	6	IIR0	r/w	Interrogator(0) Information Register
0x80080000	8	ICR0	r/w	Interrogator(0) Challenge

Hex Address	Decimal offset Address in FPGA	Register Name	Type	Description
				Register
0x800A0000	10	TIR0	r/w	TxP(0) Information Register
0x800C0000	12	TDR0	r/w	TxP(0) Delay Register
0x800E0000	14	TKR0	r/w	TCC(0) Key Register
0x80100000	16			Reserved
0x80120000	18	TIR1	r/w	TxP(1) Information Register
0x80140000	20	TDR1	r/w	TxP(1) Delay Register
0x80160000	22	TKR1	r/w	TCC(1) Key Register
0x80180000	24	ACPC	R	Antenna ACP Count Register
0x801A0000	26			Reserved
0x801C0000	28	IIR1	r/w	Interrogator(1) Information Register
0x801E0000	30	ICR1	r/w	Interrogator(1) Challenge Register
0x80200000	32	IIR2	r/w	Interrogator(2) Information Register
0x80220000	34	ICR2	r/w	Interrogator(2) Challenge Register
0x80240000	36			Reserved
0x80260000	38	VERSION	r	FPGA code version number
0x80280000	40	TR1	r/w	Test Register 1 used for testing
0x802A0000	42	TR2	r	Test Register 2 is the inverse of TR1
0x802C0000	44			Reserved
0x802E0000	46	IIR3	r/w	Interrogator(3) Information Register
0x80300000	48	ICR3	r/w	Interrogator(3) Challenge Register
0x80320000	50	TIR2	r/w	TxP(2) Information Register
0x80340000	52	TDR2	r/w	TxP(2) Delay Register

Hex Address	Decimal offset Address in FPGA	Register Name	Type	Description
0x80360000	54	TKR2	r/w	TCC(2) Key Register
0x80380000	56			Reserved
0x803A0000	58	TIR3	r/w	TxP(3) Information Register
0x803C0000	60	TDR3	r/w	TxP(3) Delay Register
0x803E0000	62	TKR3	r/w	TCC(3) Key Register

4.6.2 Lookup Table and Targets Configuration information

The DSP maintains two mirrored look-up tables and uses them in ping-pong style (as illustrated in Figure 4.7). One table is used to configure the TxP-TCC pairs in the FPGA at each ACP interrupt while the other table is being updated to prepare for the next antenna rotation, which is indicated by an ARP interrupt.

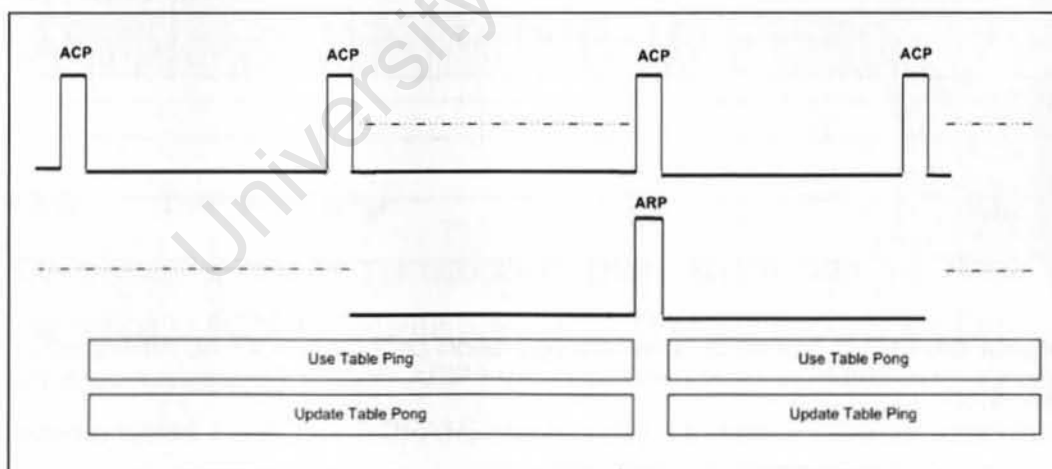


Figure 4.7 : Target information look-up tables ping-pong usage illustration

The look-up table structure is defined in Table 4.9 below.

Table 4.9 : Target configuration look-up table format. For each ACP index, configuration parameters for four TxP-TCC pairs can be maintained, allowing the emulation of $4096 * 4 = 16384$ targets per antenna rotation, thus exceeding the 1500 targets system required. The configuration parameters are valid for one antenna rotation, i.e. 360° .

ACP Count	Targets TxP-TCC Pair Configuration Parameters				
0	TxP-TCC0	TxP-TCC1		TxP-TCC2	TxP-TCC3
	Parameter	Size
	SIF Enable/Disable	32bits
	Mode 4 Enable/Disable				
	Mode 4 Decryption Key				
	SPI Enable/Disable				
	Emergency Enable/Disable				
	A Code				
	B Code				
	C Code				
	D Code				
	Reply Delay				
1	TxP-TCC0	TxP-TCC1		TxP-TCC2	TxP-TCC3
...	...				
...	...				
4095	...				

Targets created in the code have configuration parameters as summarised in Table 4.10.

Table 4.10 : Target information structure format. For each target created, the information in the table has to be provided once, and thereafter the procedures used to update the look-up tables maintain the target's mobility and use the target information in the updating process.

Target(x)
ACP Range Start
ACP Range End
ACP Change Rate
A Code
B Code
C Code
D Code
Mode 4 Decryption Key
Reply Delay
Delay Change Sign (target opening or closing from the interrogator)
Delay Change Value (how fast is the target opening or closing from the interrogator)
Emergency Enable/Disable
Mode 4 Enable/Disable
SIF Enable/Disable
SPI Enable/Disable

4.6.3 DSP SW Design

SW running on the TI TMS320C6416 DSP interacts with the FPGA by responding to ACP/ARP interrupts where the DSP re-configures the TxP-TCC pair's personalities for each ACP interrupt. The DSP maintains two mirrored look-up tables existing in SDRAM, which contain the configuration parameters of the targets. The DSP is also responsible for configuring the FRUIT interrogators.

4.7 Additional System Design Considerations and Notes

The design of the interrupt mechanism between the DSP and FPGA can be expanded to allow it to accept up to 32 different interrupt types. This is handled by the interrupt controller block in the FPGA and the interrupt mask, pending and clear registers.

There is no need for individual TxP-TCC interrupts (triggered by receiving individual interrogations) to be connected to the DSP, as this may result in bursts of interrupts that may require special attention in order to ensure that the system maintains its real-time performance. Instead, the system design has bypassed this problem by allowing interrupts to occur only in response to ACP/ARP pulses, and the statuses of all TxP-TCC pairs to be updated thereafter by the DSP at each ACP interrupt, regardless of the fact that the TxP-TCC pairs may have not received interrogations in that ACP. If a target does not exist during a specific ACP, the DSP disables it from replying by disabling the corresponding bit in the appropriate register.

The data transferred at each ACP interrupt (which refers to the personality configuration registers of the TxP-TCC pairs) is relatively low, being around 120 bytes. A simple asynchronous memory interface between the DSP and the FPGA has thus been chosen instead of a high data rate synchronous interface (which requires FIFOs and FIFO status monitoring logic in order to safely operate).

The 100 MHz clock provided to the FPGA from the DSP is suitable for the design (as discussed in Section 4.4.1), which eliminates the need for the use of the on-board PLL. Using a higher frequency clock would have had unnecessary FIFO memory resource implications when sampling and storing replies from the TxP-TCC pairs.

The use of FIFOs in the design to store and delay replies from targets is more economical than passing the replies to shift registers, due to the fact that the replies may be delayed for periods of up to around 4 ms (with a length of over 20 μ s for a mode 1 emergency reply), and the FPGA does not have enough flip-flops to implement such shift register delays.

The design is sufficiently robust to accept non-uniform ACP pulse trains, which may occur due to the antenna being installed in a windy environment. The design will however not attempt to simulate such environmental effects.

4.8 Summary

This chapter has explained the detailed system design of the FPGA and DSP. Register interfaces and SW structures defined in this chapter will be used as a guideline for the system implementation, which will be covered in the following chapter.

University of Cape Town

5. Chapter 5: System Implementation

This chapter aims to cover the implementation of the FPGA and DSP of the SSR/IFF emulator. The use of FPGA rapid prototyping tools, VHDL co-simulation, DSP SW implementation methodology, as well as portability concerns will also be covered. DSP and FPGA resource utilization and spare capacity figures are presented. Finally, the observed system limitations of the SSR/IFF target emulator will be discussed.

5.1 FPGA Design Implementation

The subsections below discuss the implementation of the FPGA used in the SSR/IFF emulator.

5.1.1 FPGA Implementation Tool-Chain

VHDL co-simulation with Modelsim [10] has been used in the Matlab/Simulink environment, for the implementation and debugging of the FPGA design. Figure 5.1 presents the implementation workflow. Since co-simulation is adequate for rapid prototyping and VHDL debugging of a non DSP intensive application, the use of HW in-the-loop debugging techniques and Xilinx System Generator was unnecessary for the implementation of the emulator. VHDL has been chosen, because the Quixote sample projects supplied are written in VHDL, and because there is more support for VHDL in South Africa than for Verilog. ChipScope from Xilinx has been used to conduct the real-time debugging of the FPGA-DSP asynchronous memory interface because of the relative difficulties that may arise when attempting to simulate the DSP's memory access to the FPGA using VHDL. Xilinx ISE version 10.1 has been used for VHDL synthesis, translation, mapping, placing and routing, for generating the programme file, as well as for managing the JTAG configuration of the FPGA.

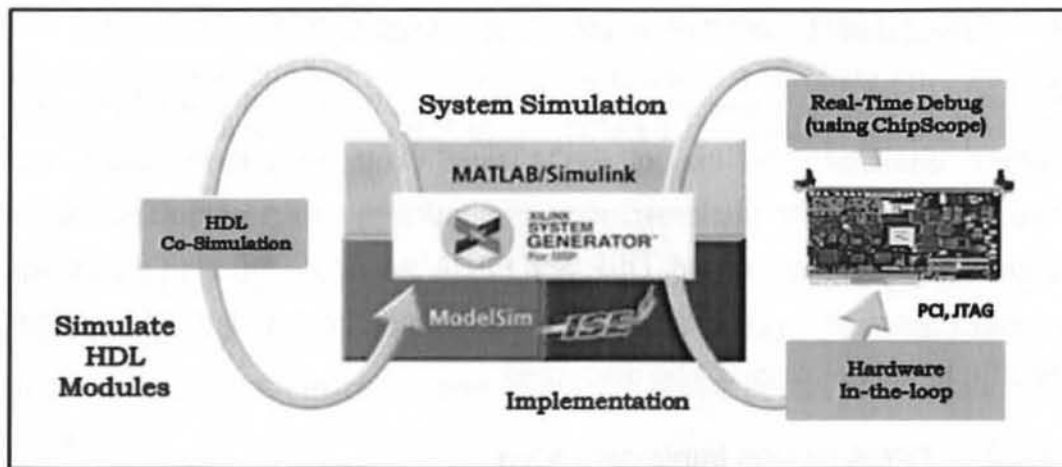


Figure 5.1 : From [9]. Simulink VHDL co-simulation, HW in-the-loop and real-time debugging. VHDL co-simulation allows the use of MATLAB code or Simulink models as a test bench, which generates stimulus for a VHDL simulation. It additionally allows multiple VHDL components to be replaced with MATLAB code or Simulink models, thus enabling the complete system to be simulated before all the VHDL design elements are available [9] [11].

5.1.2 Matlab/Simulink FPGA Implementation, Co-Simulation and Rapid Prototyping

The emulated TxP was initially implemented in Simulink by using low level components such as counters and S-R flip-flops. This approach was however complex and time-consuming because the results thereof do not map directly to the desired state-machine VHDL implementation style. Figure 5.2 presents the Simulink implementation of a pulse width discriminator block in the TxP, for example.

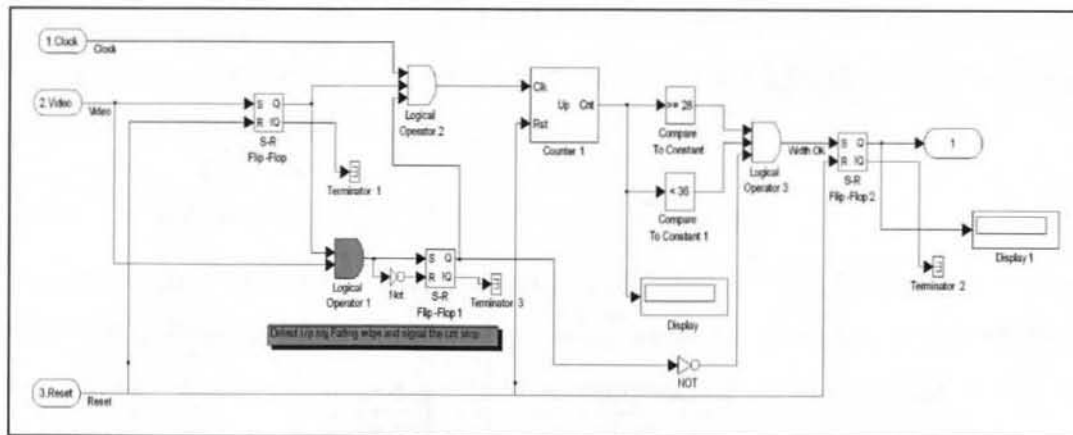
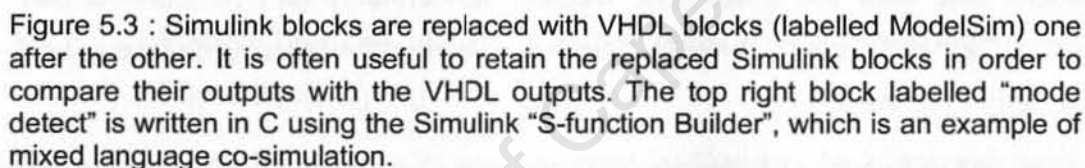


Figure 5.2 : Simulink implementation of a pulse width discriminator.

Matlab M-Files, C blocks and event-triggered Simulink blocks were later used instead of low level components, which made it simpler to write VHDL to describe the design. Simulink blocks were subsequently replaced with VHDL blocks one after the other. The model's functionality can be continuously verified as each block is replaced, thus allowing for rapid prototyping and debugging of the VHDL.

Once all the Simulink blocks are replaced with VHDL, the Simulink blocks are used to provide a test bench for the VHDL. Writing VHDL test benches is often more time consuming and complex than writing the code being tested. Using Simulink blocks to co-simulate VHDL has proved to be extremely useful for verifying the timing requirements, and it can be effectively used when testing, as will be discussed in Chapter 6. Figure 5.3 is an example of Simulink blocks being replaced with VHDL blocks, thus allowing for rapid prototyping of the TxP subsystem.



The implemented VHDL code is chip independent and generic, except for the FIFO FPGA components thereof. Should it be necessary to port the code to another FPGA manufacturer, the FIFO component declaration and port map will only require minor modification in order to comply with a different manufacturer's library calls for using on-chip FIFOs.

The sections below discuss the DSP SW implementation.

TI CCS version 3.3 allows the DSP to be programmed by means of C or C++. The SW has been written in C because of its relative simplicity and to allow for future compliance with the C coding standards of the Motor Industry

Software Reliability Association (MISRA) [18]. The IDE from TI (CCS) was supplied along with the Quixote board, and this was used for SW editing, compilation, linking and JTAG programming/debugging.

5.2.2 SW Portability

The DSP SW has been designed and implemented without the use of the DSP BIOS [19] Operating System (OS) to allow for possible future MISRA compliance and portability to a different processor. Furthermore, the C and H files that comprise the SW were partitioned into physical and application layer files. Physical layer files contain code to access any low level chip specific registers, whereas application layer files contain target information and information on look-up table maintainability (which does not involve interaction with any DSP peripherals). This partitioning allows the SW to be ported to any chip by a different manufacturer without any modification being made to the application layer files.

5.2.3 DSP Interrupt Vector Table and Memory Command File Creation

In order to develop the SW for the DSP in CCS, an interrupt vector assembly file and a memory command file must be part of the SW project. The interrupt vector file serves the linker because it contains the C function names of interrupt service routines to which the program counter should jump to if an enabled interrupt occurs. The memory command file contains instructions in respect of program sections and stack placement in the various internal or external memories available to the DSP. Memory range values were provided from the Quixote manuals [9].

5.3 FPGA and DSP Source Code

The source codes for the FPGA and DSP are on a CD accompanying this thesis. The CD directory structure is presented in Appendix B.

5.4 FPGA and DSP Resource Utilization

The figures below present the FPGA and DSP resource utilization of the current implementation. These figures are necessary to assess the possibility of porting the design to a different board or using different processors.

Device Utilization Summary				
Logic Utilization	Used	Available	Utilization	Note(s)
Total Number Slice Registers	5,883	67,584	8%	
Number used as Flip Flops	5,835			
Number used as Latches	48			
Number of 4 input LUTs	7,740	67,584	11%	
Logic Distribution				
Number of occupied Slices	6,615	33,792	19%	
Number of Slices containing only related logic	6,615	6,615	100%	
Number of Slices containing unrelated logic	0	6,615	0%	
Total Number of 4 input LUTs	9,774	67,584	14%	
Number used as logic	7,605			
Number used as a route-thru	2,034			
Number used as Shift registers	135			
Number of bonded IOBs				
Number of bonded	550	824	66%	
IOB Flip Flops	4			
IOB Master Pads	1			
IOB Slave Pads	1			
Number of RAMB16s	15	144	10%	
Number of MULT18x18s	8	144	5%	
Number of BUFGMUXs	4	16	25%	
Number of DCMs	2	12	16%	
Number of BSCANs	1	1	100%	
Number of RPM macros	12			

Figure 5.4 : FPGA resource utilization summary produced by Xilinx ISE version 10.1. The reply delay methodology used in the emulator design relies on on-chip memory (FIFOs). Only 10% of the available RAM16s of the FPGA is used for the emulation of 4000 targets. Additionally, only 8% of the available flip-flops is used, which may motivate the porting of the design to a smaller FPGA.

```
*****
TMS320C6x COFF Linker PC v6.0.8
*****
>> Linked Mon May 17 16:32:02 2010

OUTPUT FILE NAME: <./Debug/Quixote_DSP.out>
ENTRY POINT SYMBOL: "_c_int00" address: 00035460

MEMORY CONFIGURATION
```

name	origin	length	used	unused	utilization
VECTOR	00000000	00000200	00000200	00000000	100%
ON-CHIP	00001200	000aee00	000344a0	0007a960	30%
CACHE_L2	000c0000	00040000	00000000	00040000	0%
Ext_SDRAM	a0000000	02000000	00140110	01ebfef0	3%

Figure 5.5 : DSP internal and external memory utilization summary produced by CCS version 3.3. The target look-up tables are defined in the code to reside on the external SDRAM. Only 3% of the SDRAM is used and 30% of the on-chip RAM, which mainly contains the program text.

5.5 Additional Implementation Considerations

In order for the project to compile using Xilinx ISE version 10.1, the FPGA UCF file supplied along with the Quixote board (which lists the constraints in respect of pin allocation, timing, area, etc.) needed to be modified. This involved removing all the references to any unused signals or components in the file. However, this was not a problem in ISE version 9.0.

In order to reduce the board's power consumption and heat dissipation, as well as to avoid abnormal behaviour of chips connected to the FPGA that were not used in the design, unused pins have either been connected to ground or tri-stated in the FPGA.

5.6 System Limitations

The following list summarises the observed system limitations:

1. The implemented TTL solution does not allow for amplitude variations of reply pulses based on target range.
2. Recalling the ping-pong architecture in the FPGA presented in Section 4.5 and depicted in Figure 4.3, if the system interfaces with an antenna

with a faster rotation period, the system maximum simulated range will decrease (since the ACP spacing decreases as a consequence thereof). This is only a future risk, which will arise if the system is required to interface with a faster rotation period antenna. However, the implemented system is currently compliant with the 8s antenna rotation period specified by the user.

3. The functionality of the ICC has been studied and requirements have been allocated thereto, although they were not implemented. This is because the ICC was deemed to be beyond the top level project scope depicted in Figure 1.1. The secure mode 4 FRUIT replies capability of the system was satisfied without the ICC, because the interrogator being tested is not exposed to the interrogations causing FRUIT, as it is only interested in the mode 4 FRUIT replies. Therefore fixed mode 4 challenges are generated by the FRUIT interrogators.

5.7 Summary

This chapter has discussed the issues pertaining to the implementation of the FPGA and DSP, and presented the tools used to prototype and implement the design. The SW implementation methodology and portability has also been discussed. A discussion of the limitations of the SSR/IFF target emulator concludes the chapter. The next chapter aims to cover the verification and testing of system requirements.

6. Chapter 6: System Testing and Results

This chapter will cover the requirements verification and testing of the SSR/IFF targets emulator. In this regard, tests were designed to verify selected key system requirements (as set out in Chapter 3), and test results will be presented herein. The user Qualification Test Results (QTR) document [17] captures the test results not presented in this thesis for space limitations.

Two testing methods were utilised, i.e. Matlab/Simulink co-simulation and on-target tests. Each testing method will be explained below. For each test, the requirements to be verified are stated, and settings required to perform the test are presented, followed by a summary discussing the results.

6.1 System Demonstration and Testing Methodology

At the time this chapter was written, the interrogator signal processor (recall Figure 4.2) and the SSR/IFF antenna were unavailable. An emulated interrogator on the FPGA will thus act as the interrogator being tested, and the system will generate the ACP/ARP pulses. The SSR/IFF target emulator will be demonstrated firstly by using co-simulation techniques and secondly by using an Intronic [16] logic analyser. The emulated interrogator being tested operates in the same manner as any of the FRUIT interrogators in the system. TTL signals from the Quixote digital I/O pins are connected via a cable to a 50-pin breakout board, which allows the logic analyser to monitor the output signals. Figure 6.1 illustrates the test setup.

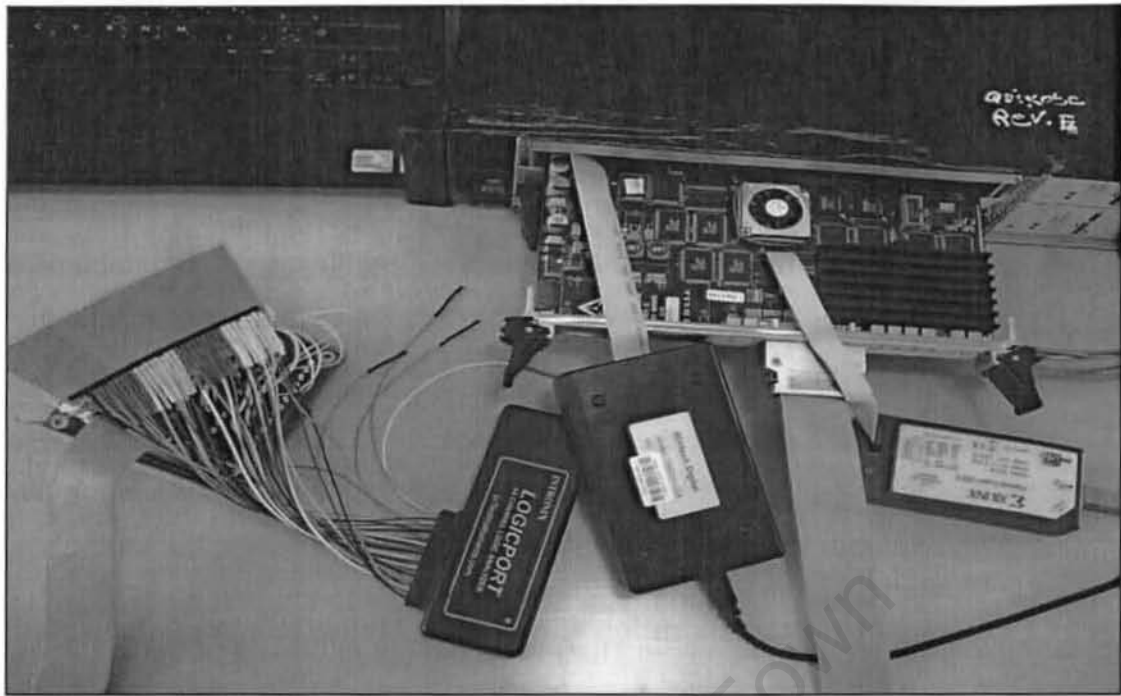


Figure 6.1 : SSR/IFF target emulator test setup. Two JTAG emulators are used for configuring the DSP and the FPGA on the Quixote board. TTL signals to/from the Quixote are routed to a breakout board for monitoring by the LogicPort Intronic logic analyser.

Co-simulation by means of Matlab/Simulink and Modelsim will be used to test the FPGA related requirements, such as pulse width validation, etc. This is due to the somewhat limited timing measurement capabilities of the logic analyser. Modelsim is an excellent visualization tool that is capable of capturing simulation results for significantly longer periods than the logic analyser is able to; moreover, the timing cursors in Modelsim are easy to use for nanosecond measurements. Using Matlab/simulink furthermore allows for more rapid testing, as test parameters such as pulse intervals, enable/disable SPI, etc can be visually edited by using a mouse pointer instead of writing VHDL test benches, as illustrated in Figure 6.3.

The limitation of the co-simulation setup is that it can only verify a single emulated target due to the absence of the role of the DSP in the simulation. In order to test multiple targets, the logic analyser is used to monitor real outputs from the system where the FPGA and DSP run in real-time. Figure 6.2 presents the co-simulation test setup in the co-simulation environment.

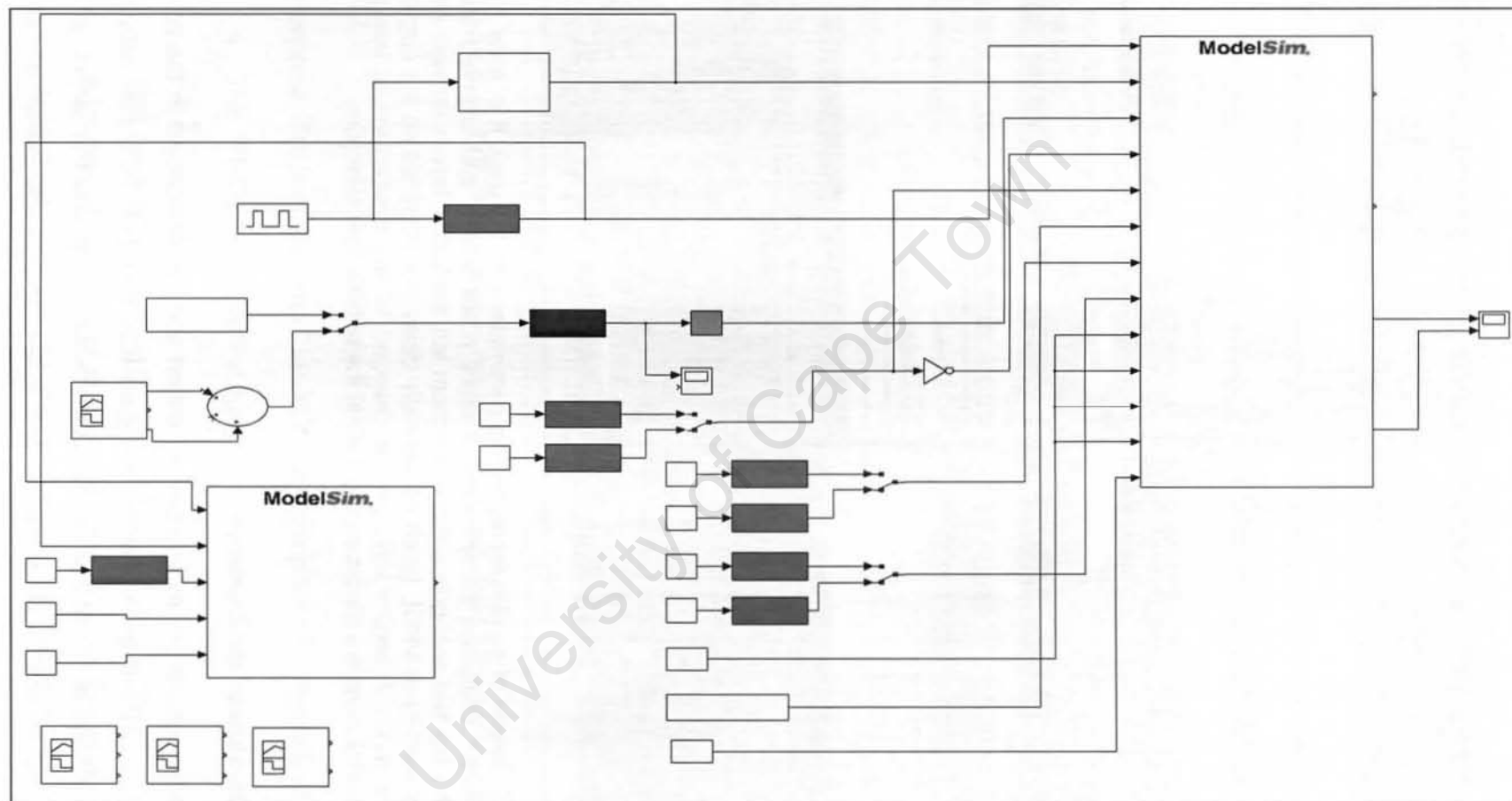


Figure 6.2 : Co-simulation TxP-TCC and FRUIT interrogator test environment. VHDL blocks are visually present in Simulink and it is fairly easy to change test parameters, such as interrogation pulse widths, interrogation modes, mode 4 keys, etc. The output of the co-simulation can be viewed with the Simulink scope or in Modelsim, where advanced timing measurement facilities are available.

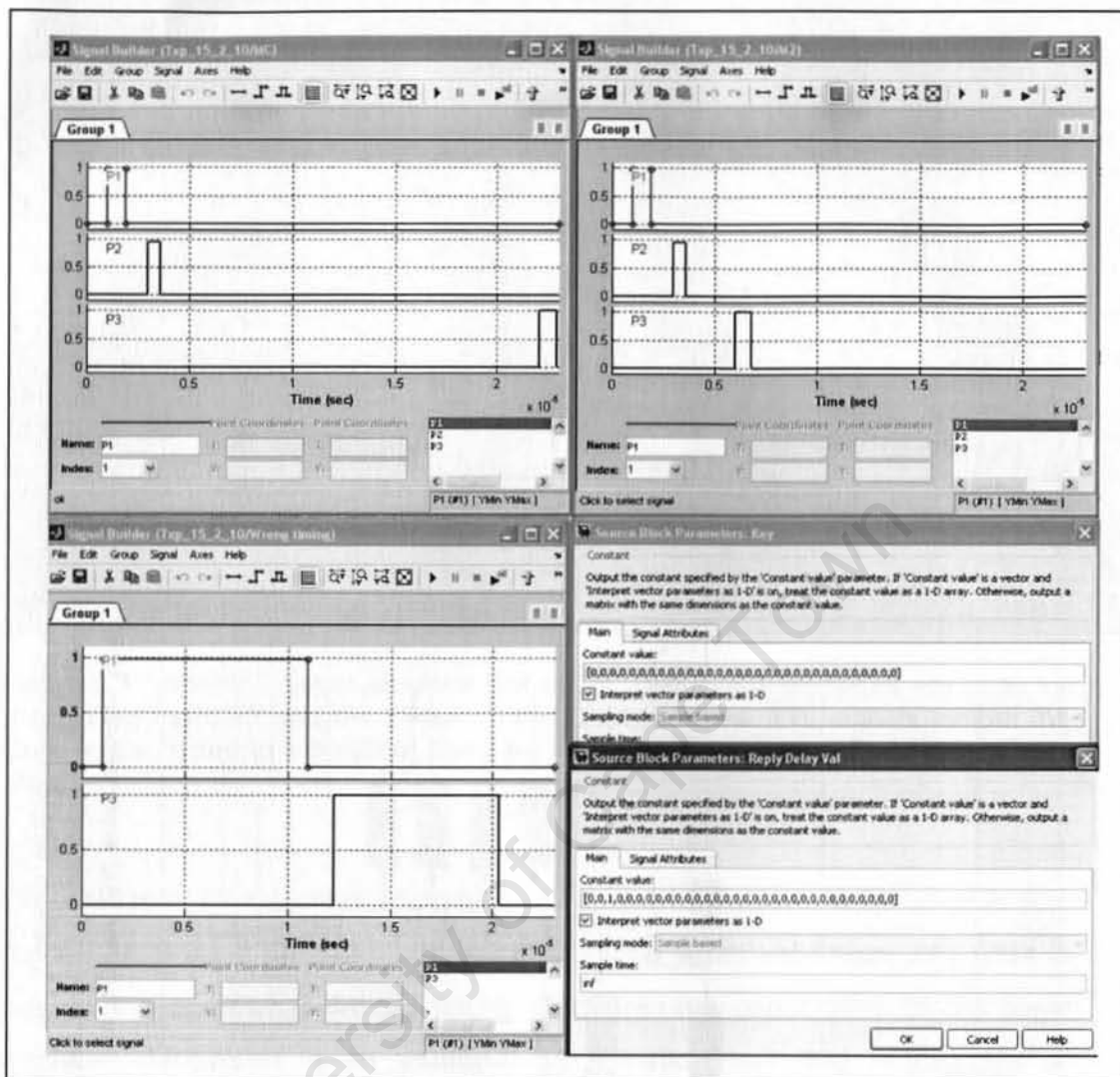


Figure 6.3 : Example of co-simulation testing parameters. In Simulink it is easy to construct different challenge modes with different pulse widths and intervals as depicted in the top two subfigures and the bottom left subfigure. Inputs defined as standard-logic-vectors in VHDL (such as the reply delay that depends on the target range and the mode 4 secure key) can be changed to any desired value, using vectors in Simulink constant blocks as depicted in the bottom right subfigure.

6.2 Co-simulation Tests

The tests shown below are mainly timing related and are performed in the co-simulation environment as presented in Figure 6.2. The TxP-TCC pair range (or the reply delay) is set to zero unless otherwise stated and the target SIF reply code bits is set to all ones for the entire test in the co-simulation environment.

6.2.1 SIF Mode Intervals

Purpose:

To verify that the TxP-TCC pair complies with P1-P3 time interval requirements as stated in Section 3.4.2.1.

Settings:

- An undefined P1-P3 SIF interval (not STANAG compliant) interrogation is sent to the TxP-TCC pair.
- SIF modes enabled, SPI disabled and emergency disabled.

Test Summary:

The TxP-TCC pair does not reply to an interrogation with an undefined P1-P3 interval. This is expected, as the TxP-TCC will only reply if the P1-P3 interval is defined.

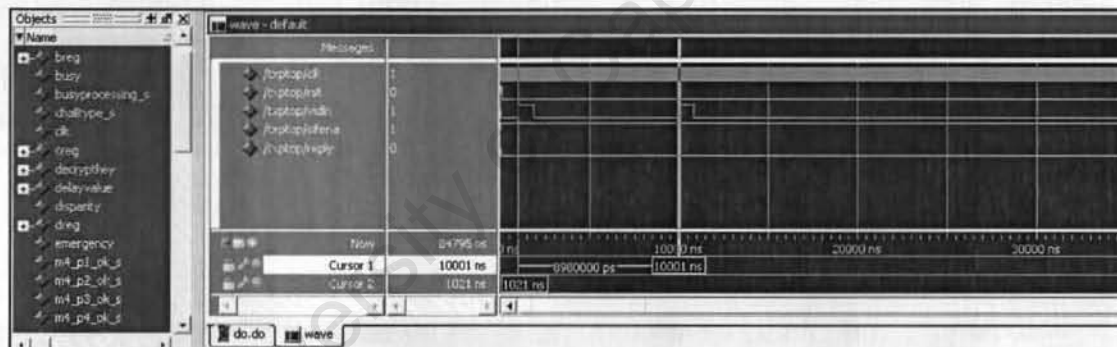


Figure 6.4 : TxP-TCC pair does not reply to an undefined SIF interrogation.

6.2.2 SIF Mode Intervals Tolerance

Purpose: To verify that the TxP-TCC pair complies with the following:

- The P1-P3 time interval tolerance requirements as stated in Section 3.4.2.1.
- TxP fixed processing time delay of 3.0 μ s with a tolerance of $\pm 0.5 \mu$ s from the rising edge of interrogation pulse P3 to the rising edge of the reply pulse F1. (This requirement is stated in Section 3.4.2.11).

Settings:

- A valid timing mode 2 interrogation is sent to the TxP-TCC pair with a negative tolerance of 0.1 μs .
- SIF modes enabled, SPI disabled, emergency disabled.

Test Summary:

As expected, the TxP-TCC pair can detect and reply to a mode 2 interrogation with a negative tolerance of 0.1 μs . The TxP complies with the $3.0 \mu\text{s} \pm 0.5 \mu\text{s}$ tolerance processing time delay requirement where a reply was produced after 3.079 μs .

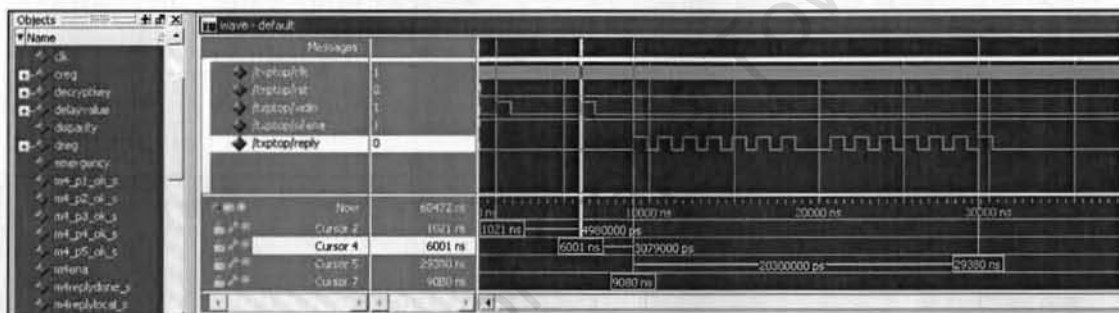


Figure 6.5 : TxP-TCC pair replies to a mode 2 interrogation with a negative tolerance of 0.1 μs with a 3 μs processing time delay.

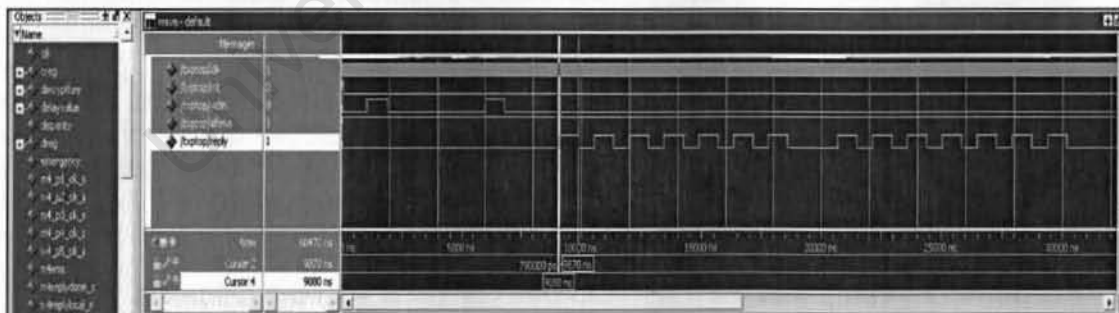


Figure 6.6 : A reply group pulse width is 0.450 μs as expected for a SIF reply.

6.2.3 SIF Mode Interrogation Pulse Width Validation

Purpose:

To verify that the TxP-TCC pair is able to validate received interrogation pulse widths in order to comply with the requirement as stated in Section 3.4.2.2.

Settings:

- A mode 1 interrogation is sent to the TxP-TCC pair containing a narrow P1 pulse.
- SIF modes enabled, SPI disabled, emergency disabled.

Test Summary:

As expected, the TxP-TCC pair does not reply to an interrogation with a pulse width outside of a $0.8 \pm 0.1 \mu\text{s}$ window period.

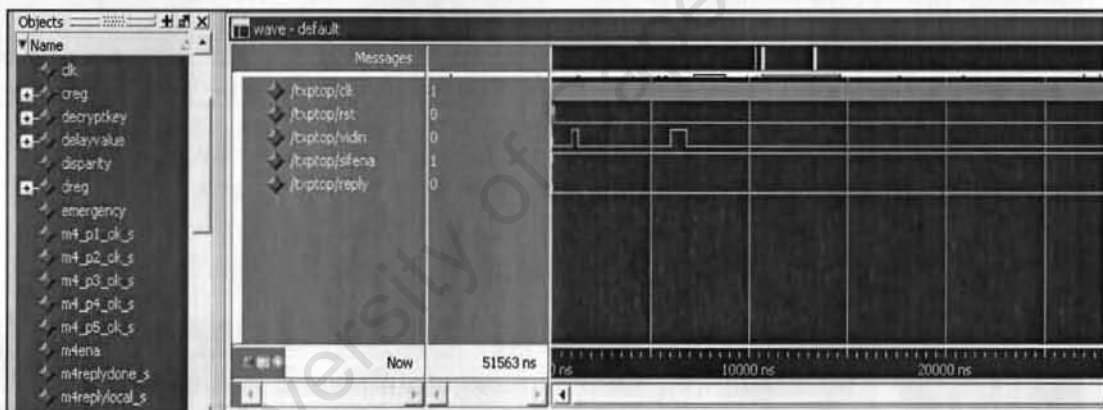


Figure 6.7 : Txp-TCC pair does not reply to a mode 2 interrogation with a narrow P1 pulse.

6.2.4 SIF Mode SPI/Emergency Replies

Purpose:

To verify the TxP-TCC pair is capable of generating SPI and emergency replies when required to do so as set out in Section 3.4.2.9.

Settings:

- A mode 1 interrogation is sent to the TxP-TCC pair.
- SIF modes enabled.

- SPI enabled, emergency disabled.
- Repeat for SPI disabled, emergency enabled.

Test Summary:

As expected, the TxP-TCC pair is capable of generating SPI and emergency replies.

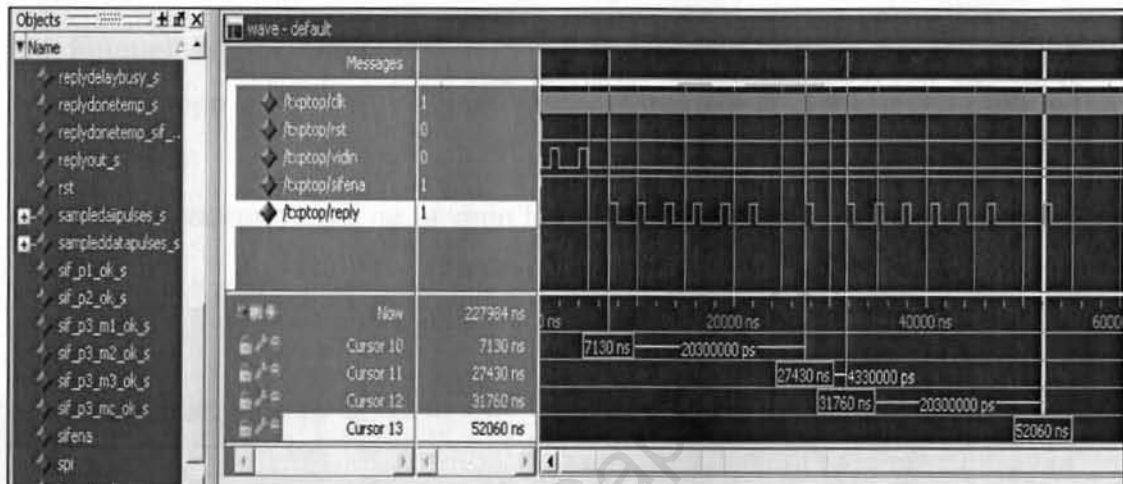


Figure 6.8 : TxP-TCC pair generating an SPI reply that comprises two reply groups for mode 1. The 20.3 μ s duration requirement from F1-F2 for each group is also satisfied.

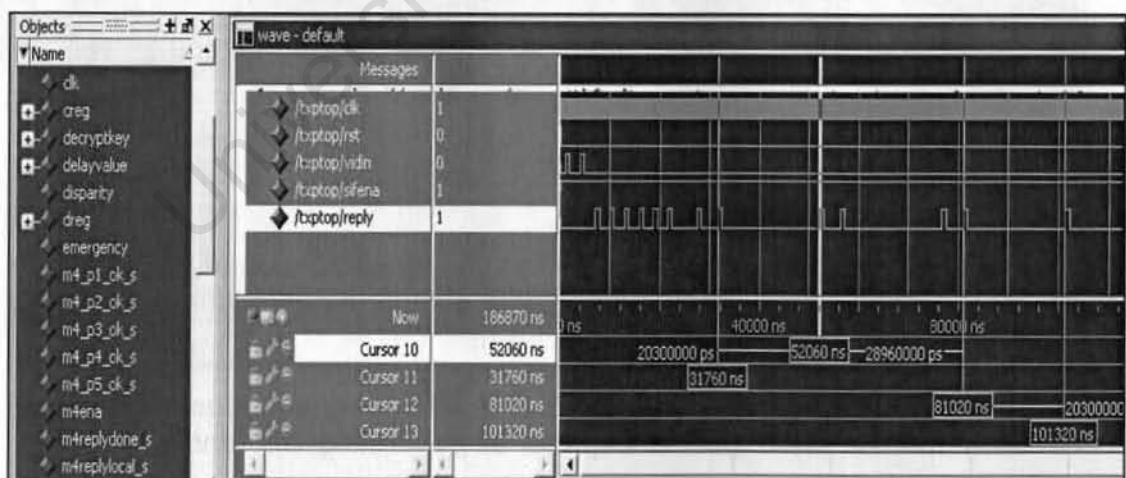


Figure 6.9 : TxP-TCC pair generating an emergency reply that comprises a reply group and three sets of framing F1-F2 pulses for mode 1.

6.2.5 Mode 4 Processing

Purpose:

- To verify that the TxP-TCC replies in the correct reply position when successfully decrypting a mode 4 challenge, as required in terms of Sections 3.4.2.12 and 3.5.2.4.
- To verify that the TxP-TCC performs All pulse validation and that it validates the widths and spacing of all received challenge pulses, as required in terms of Section 3.4.2.3.

Settings:

- A mode 4 challenge is sent to the TxP-TCC with the last reply position encrypted in the challenge, i.e. $202\text{ }\mu\text{s} + 60\text{ }\mu\text{s}$ as explained in Figure 3.6.
- A mode 4 challenge is sent to the TxP-TCC where pulses P5 and D0 are not present and All pulse 1 is missing, which creates an All rule violation.
- Mode 4 enabled, SIF modes disabled and M4 key bits set to zeros.

Test Summary:

The TxP-TCC reply occurs in the correct reply position, as the delay between P4 and the first reply pulse is measured to be $262.03\text{ }\mu\text{s}$.

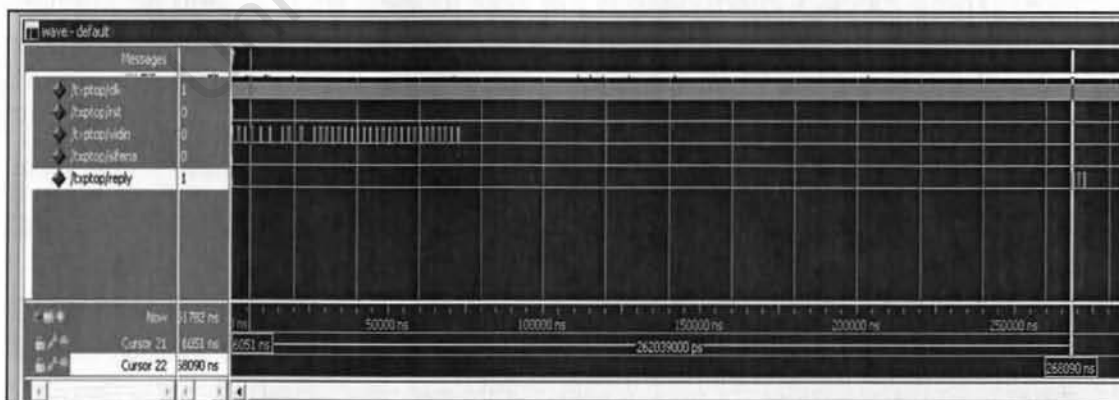


Figure 6.10 : TxP-TCC replying in the last reply position

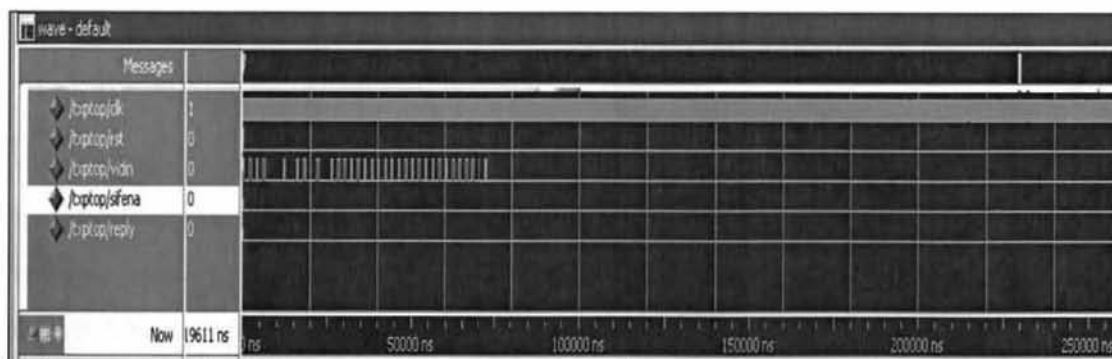


Figure 6.11 : TxP-TCC does not reply to a challenge missing the first All pulse.

6.2.6 TxP-TCC SIF/Mode 4 Internal Suppression and Performance

Purpose:

- To verify that, after the detection of a valid interrogation, the TxP-TCC ignores incoming interrogations until a reply has been generated for the detected interrogation. The TxP-TCC should be able to detect and reply to incoming interrogations within 10 μ s of the completion of the SIF reply and 290 μ s after a mode 4 reply is completed. These requirements are stated in Section 3.4.2.7
- To verify the requirements for the TxP-TCC SIF and mode 4 reply rates as listed in Sections 3.4.2.13 and 3.5.2.1. This will be done by analysis.

Settings:

- Three mode 1 interrogations are sent to the TxP-TCC with an interval of 15 μ s between them.
- Enable SIF modes.
- Repeat while enabling mode 4 and disabling SIF modes. The time interval is 150 μ s between the first and second challenges, and 125 μ s between the second and the third challenges.

Test Summary:

As expected, the TxP-TCC ignores received interrogations when a reply to a previous interrogation has not yet been generated. The TxP-TCC becomes ready to receive new interrogations even before the 10 μ s SIF and 290 μ s

secure mode readiness allowance times. This therefore proves that the TxP-TCC can easily comply with the requirements for processing 1200 and 3000 challenges per second, for SIF modes and mode 4 respectively.

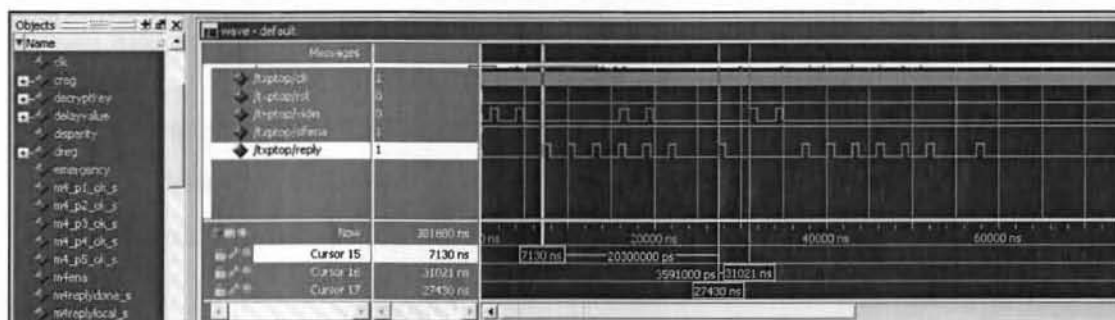


Figure 6.12 : Three mode 1 interrogations injected to the TxP-TCC. The second interrogation is ignored and the TxP-TCC was ready to reply to the third interrogation, which occurred around 3.5 μ s after the end of the reply generated for the first interrogation.

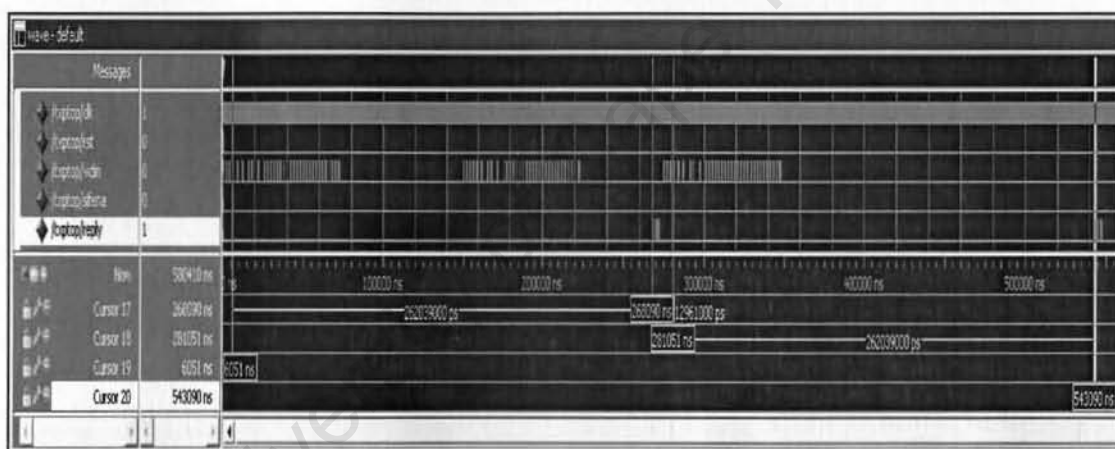


Figure 6.13 : Three mode 4 interrogations injected to the TxP-TCC. The second interrogation is ignored and the TxP-TCC was ready to reply to the third interrogation, which occurred around 2.9 μ s after the end of the reply generated for the first interrogation.

6.3 Real-Time on-Target Tests

The tests in the following subsections are performed on the target HW. The figures captured in these tests consist of screen shots from a logic analyser, whereby twelve lines are combined to represent the simulated antenna ACP count, which is then presented in decimal numbers.

6.3.1 Target Creation and Programmability Tests

Purpose:

To verify the following:

- That the system complies with the target creation and configuration requirements listed in Section 3.9.1.1.
- The requirements for the generation of ACP/ARP pulses (antenna simulation) and the system's ability to set the ACP ranges of targets, as listed under the target mobility manager, discussed in Section 3.10.2.1.

Settings:

- Create two test targets using the code settings in Figure 6.14.
- Enable two interrogators in modes 2 and 4.

```
/* create first demonstration target between ACP 10 and 60,
flying in a circle with a constant range of 100KM */
resetTargetStruct(&target1);
target1.ACPstart = 10;
target1.ACPend = 60;
target1.ACPchangeRate = 2;
target1.AReg = 0x7;
target1.BReg = 0x7;
target1.CReg = 0x7;
target1.decryptKey = 0x000000A5;
/* ( (33.3us/10ns) * 2 two way trip ) * 3us - 5 i.e (100km/FPGA clock) - 5 clocks tweak */
target1.delayValue = 66900;
target1.delayChangeSign = NEGATIVE;
target1.delayChangeValue = 0;
target1.DReg = 0x7;
target1.Emergency = 0x0;
target1.M4Ena = 0x0;
target1.SIFEna = 0x1;
target1.SPI = 0x0;

/* create second demonstration target between ACP 2000 and 2020,
flying towards the radar at a speed of 200m/s and at an initial range of 200KM */
resetTargetStruct(&target2);
target2.ACPstart = 2000;
target2.ACPend = 2020;
target2.ACPchangeRate = 0;
target2.AReg = 0x1;
target2.BReg = 0x0;
target2.CReg = 0x0;
target2.decryptKey = 0x000000A5;
target2.delayValue = 1332995;
target2.delayChangeSign = NEGATIVE;
target2.delayChangeValue = 10000; // 10us for a 200m/s target
target2.DReg = 0x0;
target2.Emergency = 0x0;
target2.M4Ena = 0x1;
target2.SIFEna = 0x0;
target2.SPI = 0x0;
```

Figure 6.14 : The code snippet presented is used to create two test targets. The system is flexible enough to create more complicated scenarios, such as, for example, crossing targets or enabling up to 4000 targets.

Test Summary:

As seen in the figures below, targets are successfully created and are configurable in identity, mode 4 key, range, velocity and azimuth. The created target ranges and azimuths are updated by the system if required (stationary targets can also be created).

University of Cape Town

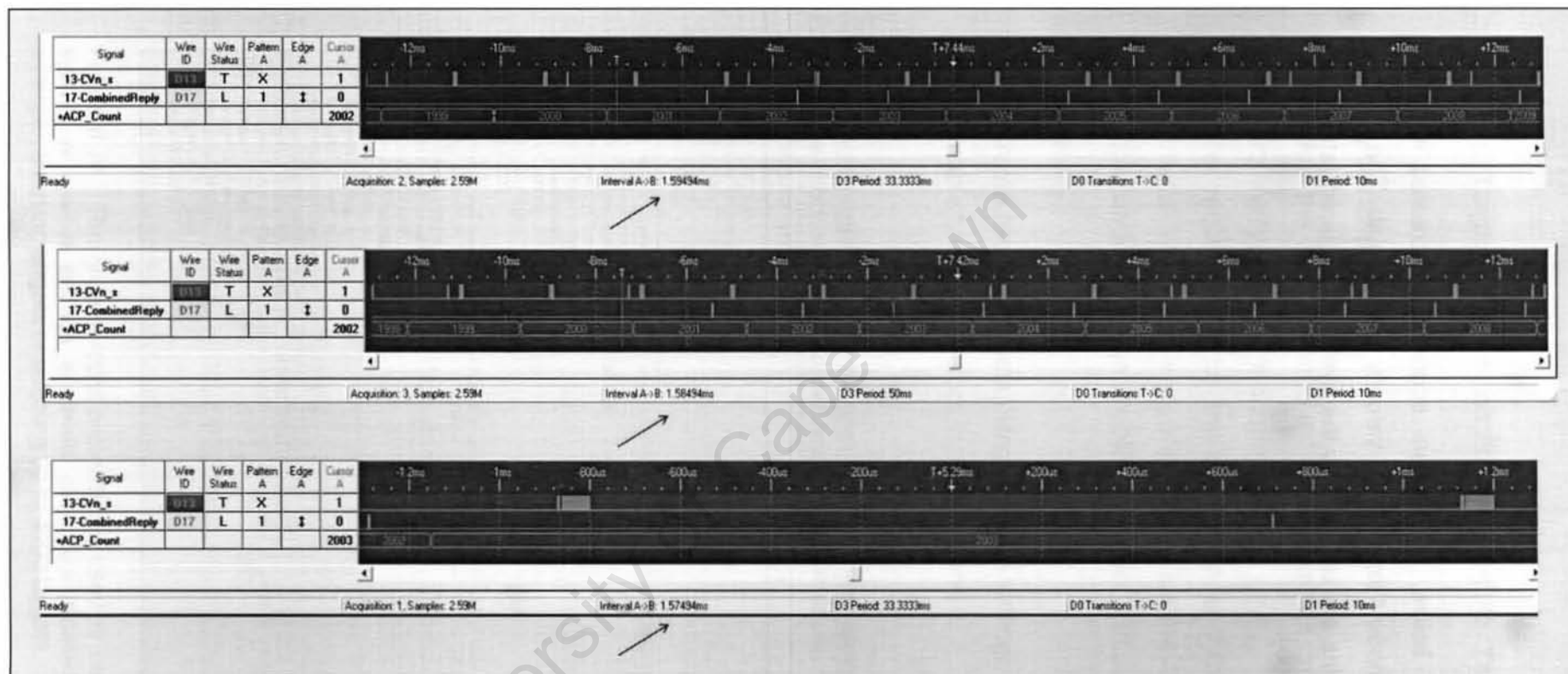


Figure 6.15 : The mode enabled target between ACPs 2000 and 2020 is flying towards the interrogator with a constant velocity of 200m/s. After each antenna rotation, the reply delay corresponding to the target range is 10 μ s less as measured by using logic analyser cursors. A delay of 1595 μ s is equal to the two-way interrogation/reply trip time for a target at 200km, plus the 202 μ s TxP-TCC processing time and the 60 μ s mode 4 last position reply delay,

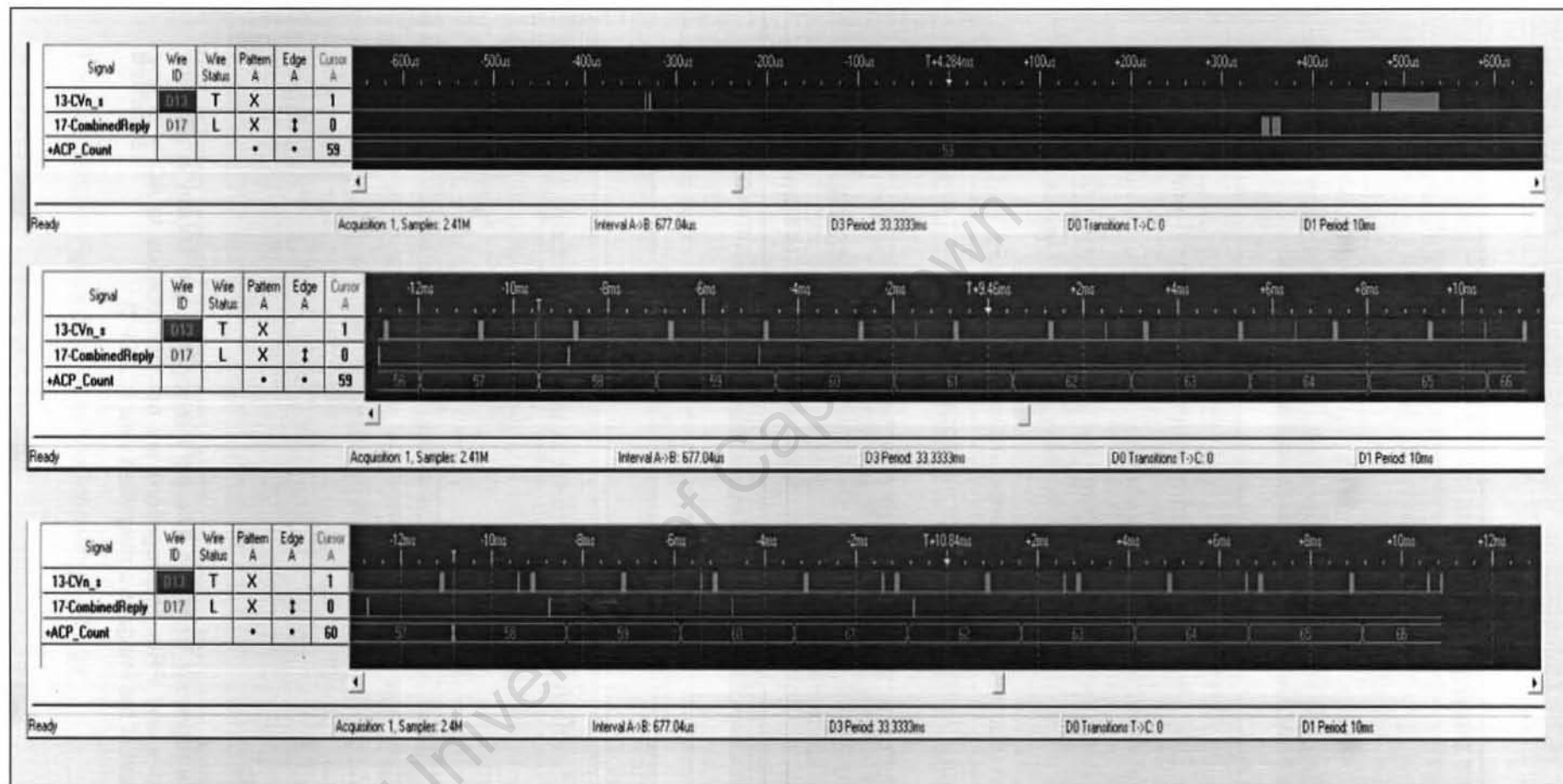


Figure 6.16 : The first target is between ACPs 10 and 60 (from Figure 6.14) with an azimuth change rate of 2 ACPs per antenna rotation. Replies from the target are present for interrogation occurring up to ACP 60 for the first antenna rotation and up to 62 for the second and so on. The upper part of the figure is a magnified view of a reply. Note that the target is only enabled for SIF modes, and that it does not reply to the mode 4 interrogations.

6.3.2 FRUIT Interrogators Test

Purpose:

The verification of the requirements for multiple interrogators listed in Sections 3.6.3.1 and 3.7.2.1.

Settings:

- From the DSP, enable FRUIT interrogator 0 for mode 1 with a PRI of 4ms, which is done by writing to the IIR0.
- From the DSP, enable FRUIT interrogator 1 for mode 4 with a PRI of 2ms, which is done by writing to the IIR1 (recall Table 4.8).
- Create an example target to demonstrate a FRUIT reply.
- Reconfigure the interrogators for interrogation in modes 1 and C.

Test Summary:

As expected, the system complies with the multiple interrogators requirement. The system is thus capable of generating FRUIT replies. FRUIT interrogators are configurable for interrogation modes and in PRI in numerous FRUIT scenarios.

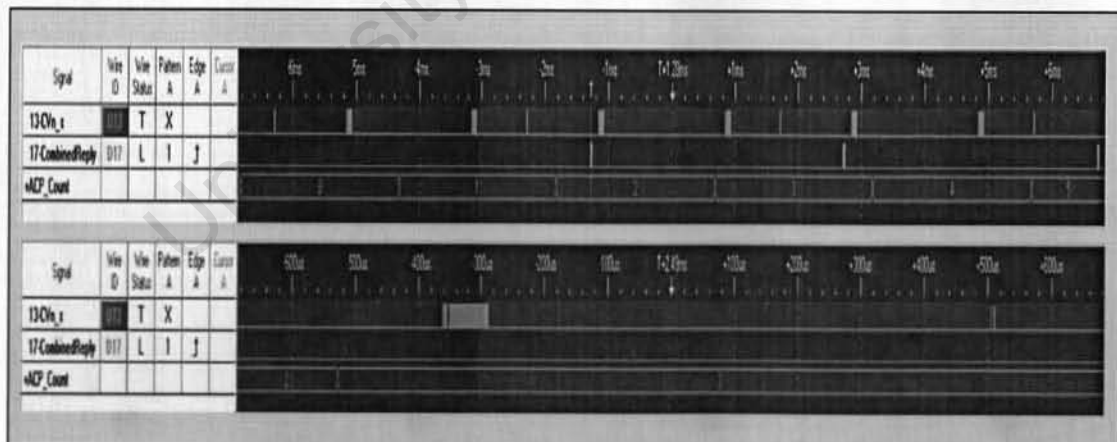


Figure 6.17 : Interrogations from two different interrogators are shown in different interrogation modes and PRIs. Interrogations are not synchronous to ACPs in any way. The lower part of the image is a magnified view of ACP 3.

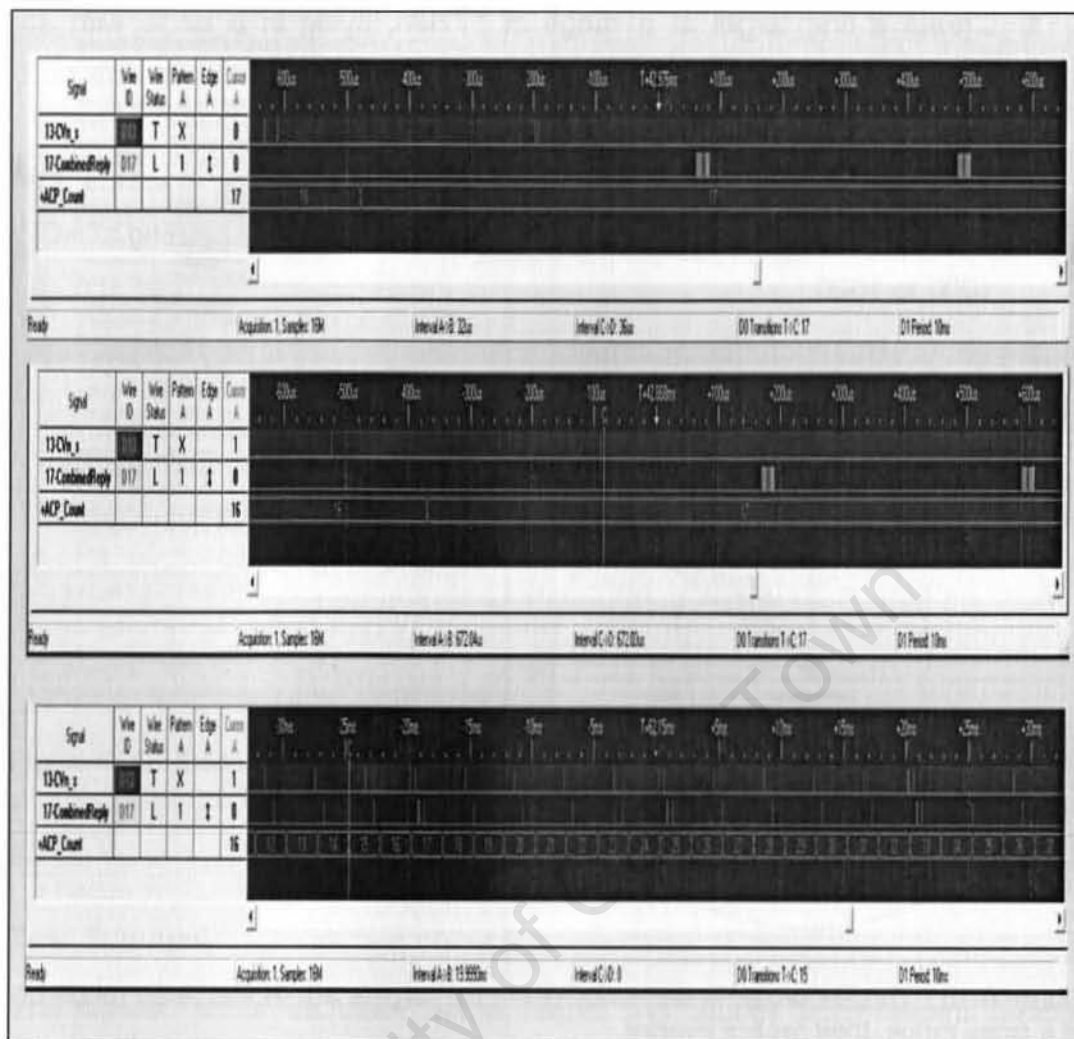


Figure 6.18 : FRUIT reply scenario. During ACP 17, the first reply is intended for the mode C interrogation generated during ACP 16, and it will thus be considered as a FRUIT reply to the interrogator interrogating in mode 1. The second reply comes from the same target and is in response to the mode 1 interrogation. The lower part of the figure is zoomed out.

6.3.3 Garbled Replies Test

Purpose:

To verify the requirement for garbled replies as stated in Section 3.6.3.2. The test will also present the system's ability to create target mobility scenarios.

Settings:

The scenario in Figure 6.19 uses the following settings:

1. Create a first target at a range of 177km, flying in a circle with an azimuth starting at ACP 927 to 992 and an azimuth change rate of 2 ACPs per antenna rotation.
2. Create a second target at a range of 200km, flying towards the interrogator with a velocity of 200m/s and at an azimuth starting at ACP 1000 to 1020.

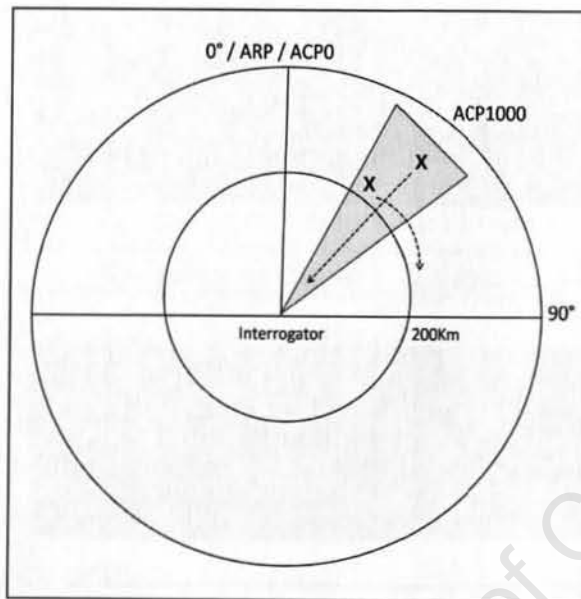


Figure 6.19 : Targets crossing scenario. When the targets are at the same range or at a close range, their replies overlap.

```

resetTargetStruct(&target1);
target1.ACPstart = 927;
target1.ACPend = 992;
target1.ACPchangeRate = 2;
target1.AReg = 0x7;
target1.BReg = 0x7;
target1.CReg = 0x7;
target1.decryptKey = 0x000000A5;
target1.delayValue = 118666;
target1.delayChangeSign = NEGATIVE;
target1.delayChangeValue = 0;
target1.DReg = 0x7;
target1.Emergency = 0x0;
target1.M4Ena = 0x0;
target1.SIFEna = 0x1;
target1.SPI = 0x0;

resetTargetStruct(&target2);
target2.ACPstart = 1000;
target2.ACPend = 1020;
target2.ACPchangeRate = 0;
target2.AReg = 0x0;
target2.BReg = 0x0;
target2.CReg = 0x0;
target2.decryptKey = 0x000000A5;
target2.delayValue = 133295;
target2.delayChangeSign = NEGATIVE;
target2.delayChangeValue = 1000;
target2.DReg = 0x0;
target2.Emergency = 0x0;
target2.M4Ena = 0x0;
target2.SIFEna = 0x1;
target2.SPI = 0x0;

```

Figure 6.20 : Code snippet used to create test targets for the garbled replies test

Test Summary:

The screen shots as seen below depict the replies from targets before crossing each other, while at close range or at the same range, and after they have crossed each other. The sequence of events is broken down and presented in the figures below. As expected, the system is compliant with the requirement in respect of generating garbled replies.

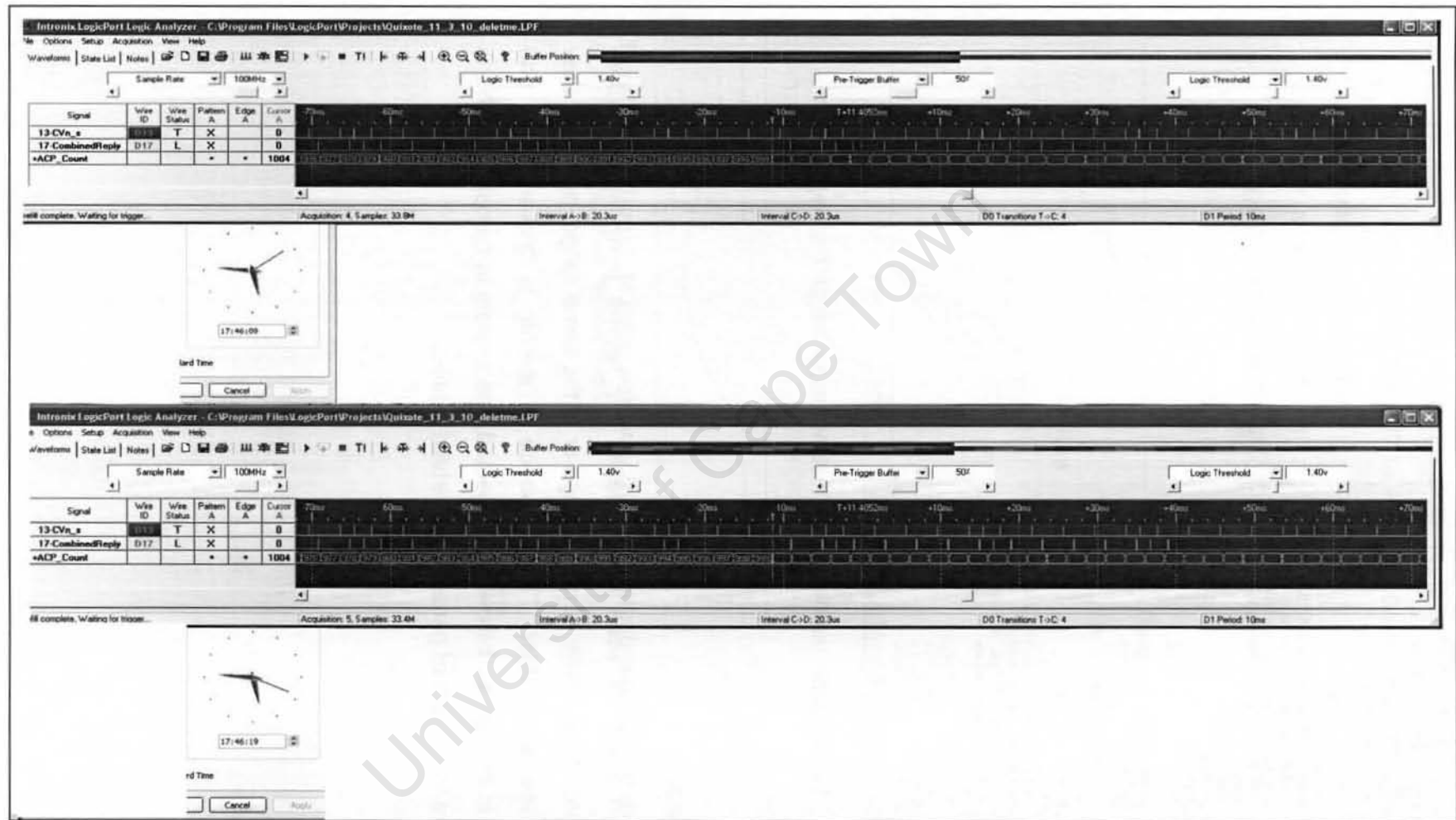


Figure 6.21 : Replies from two targets with different reply codes are presented. As the targets come closer to each other in range, their replies overlap. The sequence of events is continued in the next figures. As the targets move away from each other, the garbling condition no longer exists.

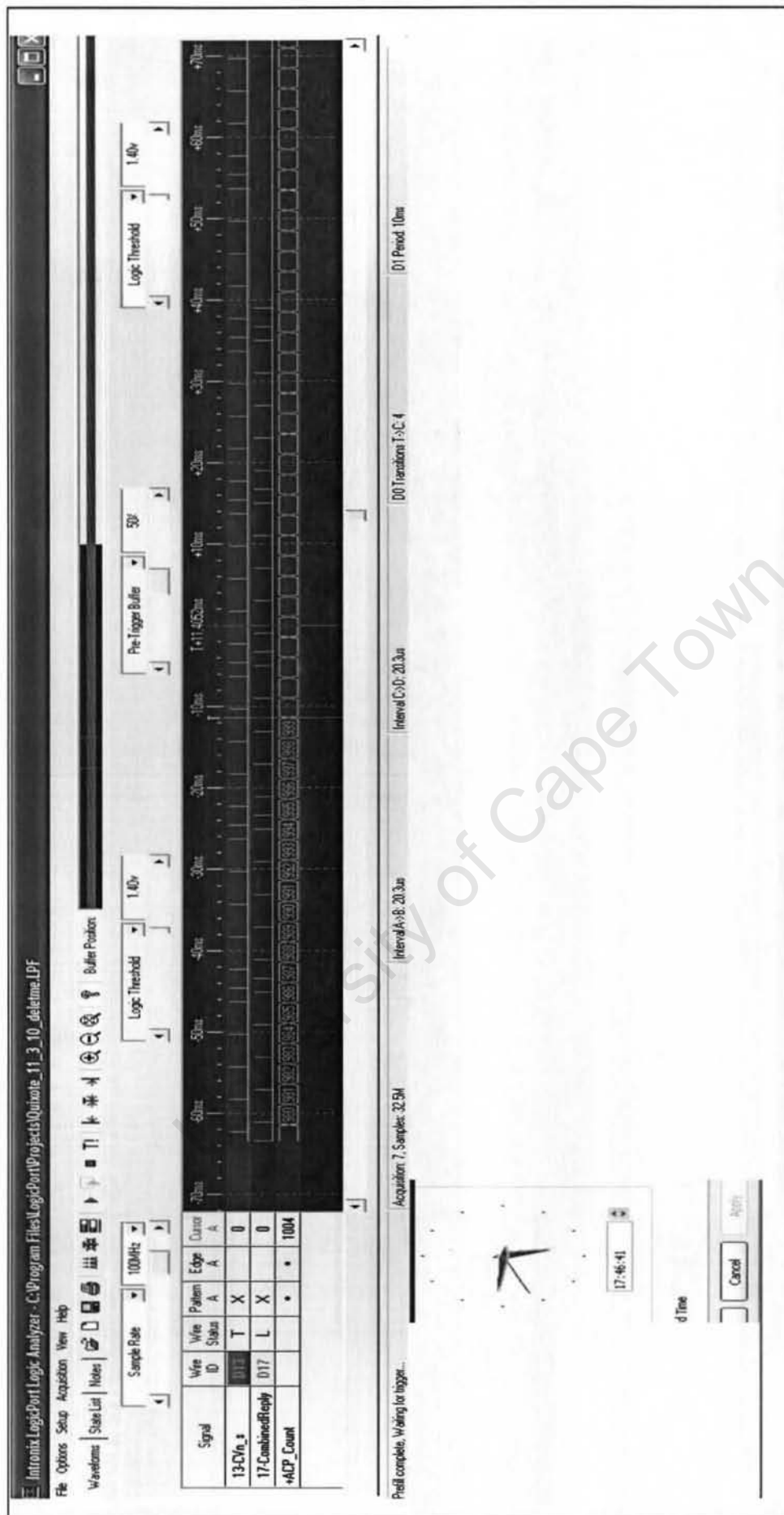


Figure 6.22 : Continued sequence of garbling test result from Figure 6.21

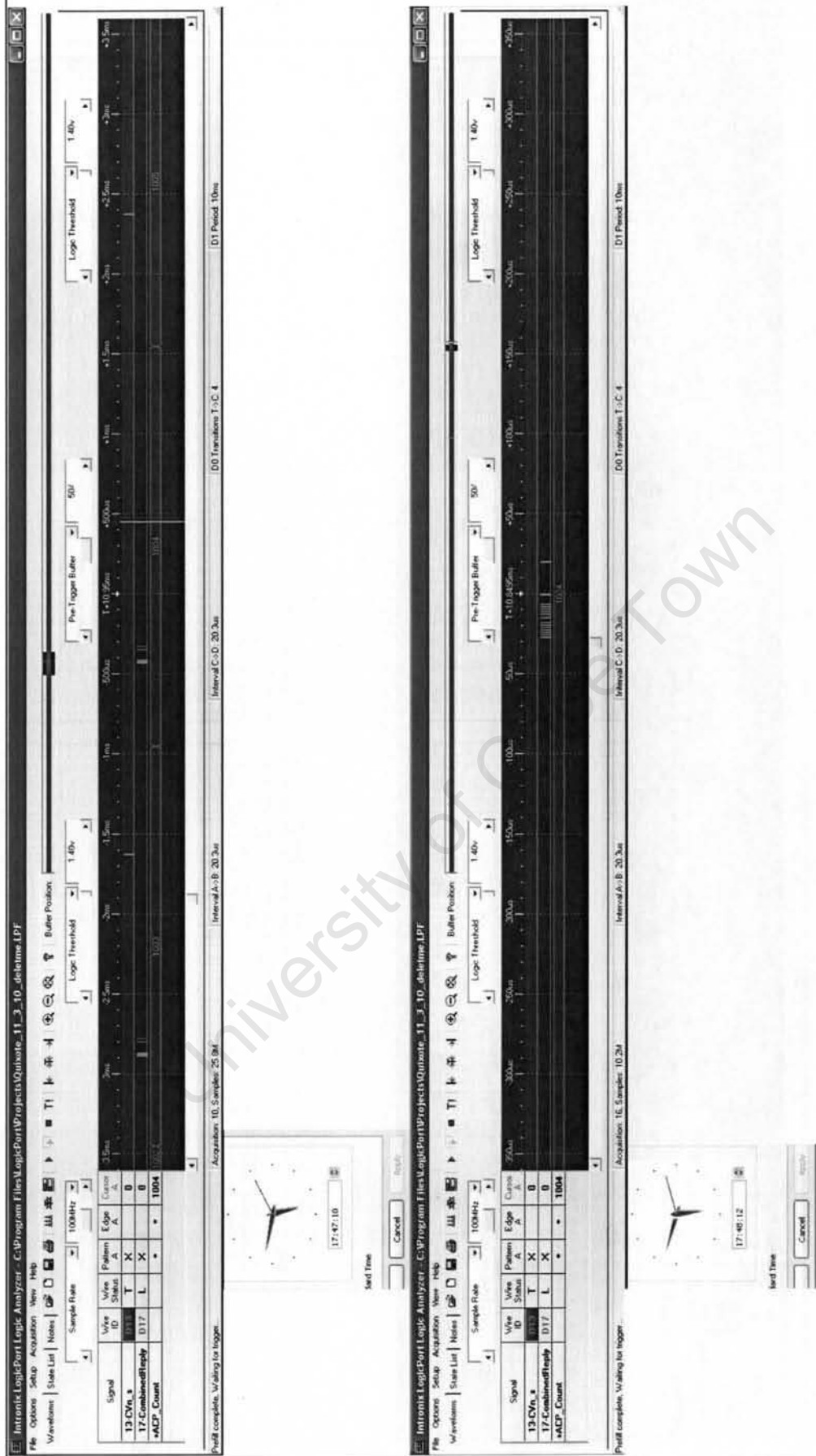


Figure 6.23 : Continued sequence of garbling test result from Figure 6.22

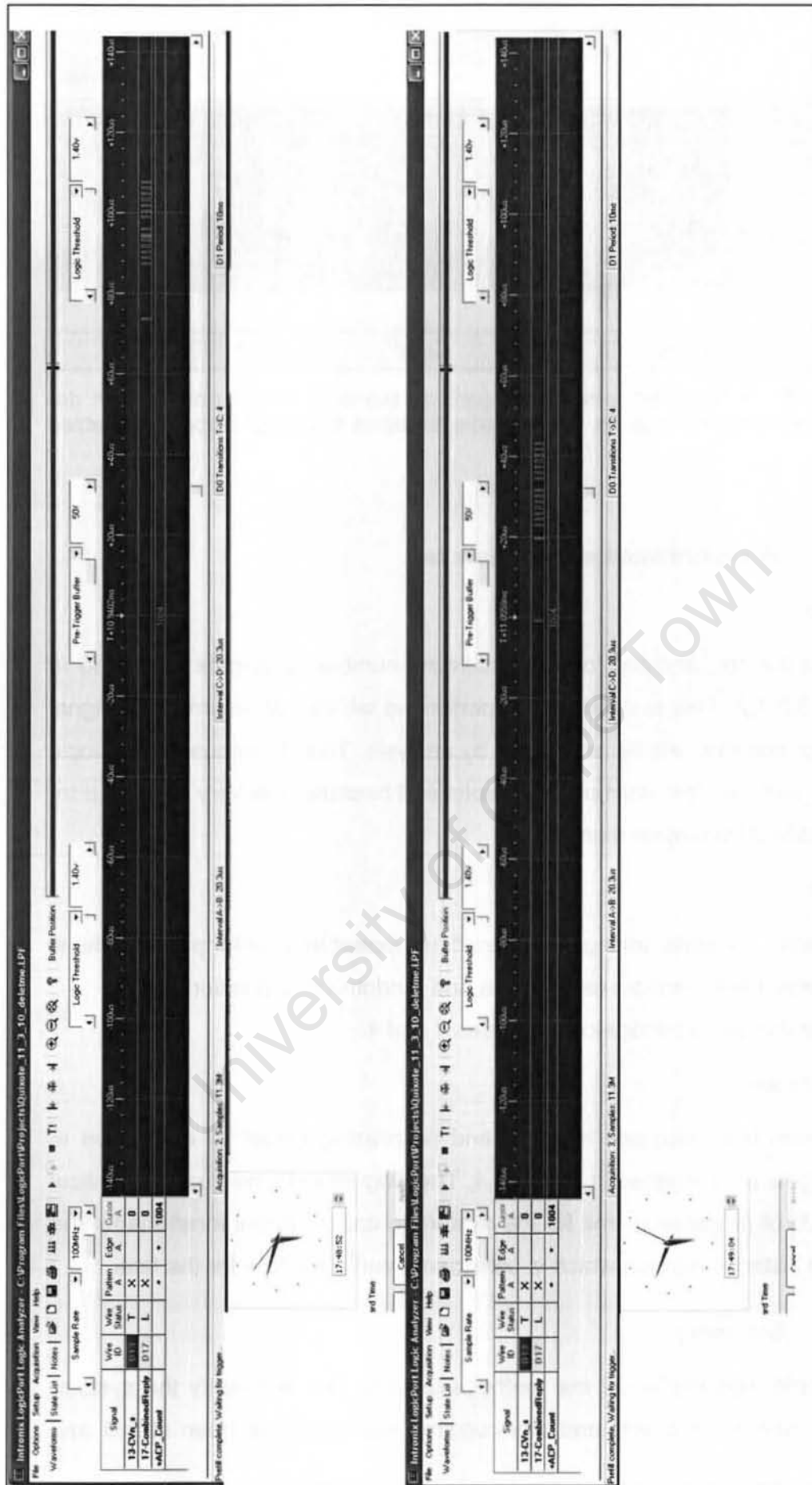


Figure 6.24 : Continued sequence of garbling test result from Figure 6.23

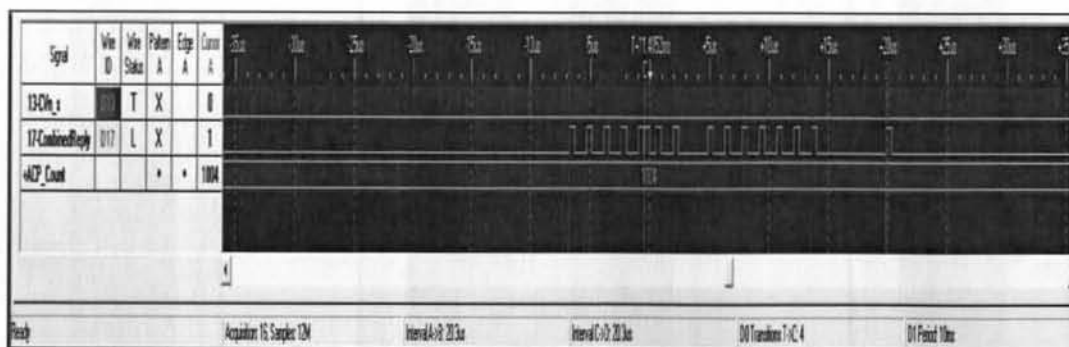


Figure 6.25 : A magnified view of the garbling scenario. An interrogator with de-garbling and tracking facilities may be able to detect the targets from the garbled replies.

6.3.4 Maximum number of targets test

Purpose:

To verify the requirement for the maximum number of targets as stated in Section 3.9.1.2. This test cannot be performed without an interrogator signal processor and thus will be performed by analysis. This is because of the logic analyser sample store memory limitations and because it is very difficult to try and identify 1500 targets manually.

Settings:

1. Using the code settings in Figure 6.14, repeat in a for-loop to enable all targets with random reply codes and random initial positions.
2. Enable two interrogators in modes 2 and 4.

Test Summary:

The system has adequate memory and processing power to enable up to 4000 targets as discussed in Chapter 4. The ping-pong techniques used allow 8 seconds of processing time for the system to update target locations for the following antenna rotation which is considered sufficient time for the task.

6.4 Summary

This chapter has explained the methods used to test and verify the system. The purpose of each test and any required settings have been stated and

their results discussed. The next chapter will conclude the project and suggest areas for future improvements.

University of Cape Town

7. Chapter 7: Conclusions and Future Work

This chapter covers the conclusions and recommendations of the SSR/IFF target emulator project, and proposes future areas of improvement.

7.1 Project Summary and Conclusions

The SSR/IFF emulator project began by capturing the user requirements in Chapter 2. These were further analysed and a system breakdown structure was drawn up from the analysis. Concept summaries for each subsystem in the system breakdown were then presented in order to facilitate requirements allocation for each of the subsystems. This resulted in a specification for the product being realized, which was examined in Chapter 3. A top-level and detailed design of the system, including tradeoffs and partitioning decisions between the FPGA and DSP, were then discussed in Chapter 4. Consequently, a description of the implementation methodology and the implantation tool-chain, followed by the limitations of the system was put forward in Chapter 5. Chapter 6 portrayed the testing and verification of the system against requirements, wherein test cases were designed and test results discussed.

It was found that the SSR/IFF target emulator is compliant with the requirements presented in Chapter 3, apart from the system limitations listed under Section 5.6. The system is capable of generating replies in real-time from 4000 distinct identity mobile targets for SSR/IFF modes 1, 2, 3/A, C and 4, situated at a distance from 0 to 600km. The system is additionally able to generate FRUIT replies and to interface with or emulate an SSR/IFF antenna. The system furthermore allows for the creation of target crossing scenarios for generating advanced garbled replies situations. The fully configurable target parameters allow for the emulation of different target types including stationary ones.

7.2 Recommendations and Future Work

Below is a list of recommendations for possible future improvements to the SSR/IFF target emulator:

1. In order to allow the system to interface with an antenna that has a higher rotation period than the one specified by the user (8s/rotation) or to emulate targets at ranges beyond 600km, a third set of TxP-TCC pairs can be added to the FPGA design. The ping-pong operation will have to be modified to create an operation involving three stages, which would allow a group of TxP-TCC pairs an amount of time to delay a reply equal to the time between four ACPs, as opposed to three in the current implementation. The DSP code will require no or only minor modification and the target information look-up tables will not be affected. Recall Figure 4.3 for the current implementation.
2. Target creation in the current implementation is done manually or by using function calls. An automated solution may involve a PC application with a GUI that will allow graphical scenario creation. This application would be able to update the target look-up tables in the SDRAM via the DSP, since the DSP is already equipped with a PCI interface peripheral, which would make it available on the PCI bus, while also allowing for a possible interface point with the ITRC for data exchange with the target emulator.
3. The resource utilization, as illustrated in Figure 5.4 and Figure 5.5 in Chapter 5, shows that the processors and memories used have ample spare capacity. The Quixote board also contains ADCs, DACs and other analogue support components, which are not utilized by the target emulator in a TTL implementation. It is recommended that the design be ported to a less expensive board if the idea in the abovementioned point is not implemented.
4. A more realistic interrogator operation environment could be provided by modifying the FRUIT interrogators in order to allow for a PRI random stagger.
5. As a future improvement, the emulator may simulate the presence of reflective surfaces during user selected ACP ranges. This would simulate the effect of multiple target returns in order to create a real life scenario to which interrogators may be exposed.

University of Cape Town

Bibliography

- [1] Stevens, M.C. (1988). Secondary Surveillance Radar. Artech House.
- [2] Military Agency for Standardization, North Atlantic Treaty Organization (NATO). (1990). Standardization Agreement (STANAG) 4193 PART 1 edition 2 Annex A and appendices, Technical Characteristics of IFF Mk XA and Mk XII Interrogators and Transponders.
- [3] Kingsley. S. and Quegan, S. (1999). Understanding Radar Systems. SciTech Publishing.
- [4] United States Navy, Naval Air Systems Command and Naval Air Warfare Centre. (1999). Electronic Warfare and Radar Systems Engineering Handbook Rev 2.
- [5] Defence Systems Management College (DSMC) Fort Belvoir. (1983). Systems Engineering Management Guide.
- [6] Blanchard, B.S. and Fabrycky, W.J. (1990). Systems engineering and analysis. 2nd ed. Prentice-Hall, Inc., Englewood Cliffs, N.J.
- [7] "Identification Friend or Foe" [Online] Available: <http://www.globalsecurity.org/military/systems/aircraft/systems/iff.htm> (Accessed in June 2010).
- [8] "Innovative Integration Quixote DSP Board Product Folder" [Online] Available: <http://www.innovative-dsp.com/products.php?product=Quixote> (Accessed in June 2010).
- [9] "Innovative Integration Frame Work Logic Product Folder" [Online] Available: <http://www.innovative-dsp.com/products.php?product=FrameWork%20Logic> (Accessed in June 2010).
- [10] Mentor Graphics Modelsim [Online] Available: <http://model.com> (Accessed in June 2010)
- [11] Mathworks matlab/simulink [Online] Available: <http://www.mathworks.com/products/simulink/> (Accessed in June 2010).
- [12] ISO31-5: Quantities and units: Electricity and Magnetism. International Organization for Standardization, (1992).
- [13] VirtexII platform FPGAs data sheet, XILINX, (2007).
- [14] Innovative Integration. (2008). Quixote User's Manual Rev 2.0.
- [15] TMS6416 DSP data sheet, TI, (2001).

- [16] "INTRONIX, PC-Based Test and Measurement" [Online] Available: <http://www.pctestinstruments.com/logicport/specifications.htm> (Accessed in June 2010).
- [17] Qualification Test Results (QTR) number 3302-7642 V1.2. (May 2010).
- [18] "Motor Industry Software Reliability Association" [Online] Available: <http://www.misra.org.uk/> (Accessed in June 2010).
- [19] "DSP/BIOS Real-Time Kernel" [Online] Available: <http://focus.ti.com/docs/toolsw/folders/print/dspbios.html> (Accessed in June 2010).

University of Cape Town

Appendix A : User Requirements Traceability Matrix

Table 7.1 : User Requirements Traceability Matrix

User Requirement Section	Description	Derived Requirement Section(s)	Relevant Aspects
2.1.1	TxP and TCC	3.4.2	<ul style="list-style-type: none"> - TxP timing requirements. - TxP interface to TCC. - TxP performance requirements.
		3.5.2	<ul style="list-style-type: none"> - TCC timing requirements. - TCC performance requirements.
2.1.2	SSR/IFF Reply Modes	3.4.2 & 3.5.2	TxP SIF modes and mode 4.
2.1.3	Number of Targets	3.9.1.2	Number of Targets
		3.10.2	Target distribution in a 360° space
2.1.4	Distinct Target Identity	3.9.1	Target configuration parameters, which include reply codes.
2.1.5	Friendly and Non-Friendly Targets	3.9.1	Target configuration parameters include a mode 4 key.
2.1.6	Real-time Operation	3.12	Real-time requirement will be satisfied by implication when the other subsystems' requirements are satisfied.
2.1.7	Continuous Operation	3.9.1	Target parameters are reconfigurable.

User Requirement Section	Description	Derived Requirement Section(s)	Relevant Aspects
		3.11.1	System will keep maintaining targets until user chooses to end the emulation.
2.1.8	Target Mobility and Space	3.10.2	Target distribution in a 360° space.
		3.9.1	Target configuration parameters include target range.
		3.9.1	Target configuration parameters include mode C altitude code.
2.1.9	Garbled and FRUIT Replies	3.6.3	Placement of interrogators in the simulated area around the interrogator being tested.
		3.7.2	<ul style="list-style-type: none"> - SSR/IFF interrogator challenge generation timing requirements. - SSR/IFF interrogator performance requirements. - SSR/IFF interrogator/ICC interface requirements.

User Requirement Section	Description	Derived Requirement Section(s)	Relevant Aspects
		3.9.1 & 3.10.2	Azimuth and range of emulated targets are configurable for the creation of FRUIT and garbling scenarios.
		3.8.2	<ul style="list-style-type: none"> - ICC timing requirements. - ICC performance requirements.
2.1.10	Antenna Interface	3.10.2	Antenna interface and simulation.
2.2	HW Requirements	3.14	Input/output pins available for <ul style="list-style-type: none"> - Receiving challenges from the interrogator being tested and the antenna. - Combined replies from the system to the interrogator being tested.
2.3	Requirements for Future Use	3.13	System to provide interface point for the ITRC.

Appendix B : Source Code

The sections below present the source code CD directory structure and contents.

The folders in the root directory of the CD are:

- FPGA
- DSP
- Simulink
- System test results images

B.1 FPGA VHDL Code

Name	Size	Type
modelsim.ini	43 KB	Configuration Settings
FIFO_d.v	6 KB	MTI verilog
EMIF A.vhd	1 KB	MTI vhd
FIFO_d.vhd	6 KB	MTI vhd
Interrogator.vhd	6 KB	MTI vhd
INTERRUPTS_CONTROLLER.vhd	4 KB	MTI vhd
interruptSource.vhd	2 KB	MTI vhd
PingPong.vhd	2 KB	MTI vhd
pulsesEval.vhd	25 KB	MTI vhd
ReplyDelayXilinx.vhd	10 KB	MTI vhd
ReplyGen.vhd	14 KB	MTI vhd
SIFreplyTrig.vhd	2 KB	MTI vhd
TopLevel.vhd	59 KB	MTI vhd
TxPtop.vhd	8 KB	MTI vhd

Figure 7.1 : FPGA subdirectory. VHDL files for the FPGA simulation and implementation

B.2 DSP C Code

Name	Size	Type
vectors.asm	4 KB	ASM File
DILUT.c	24 KB	C File
DlTimer1.c	1 KB	C File
DlVideoProcessing.c	4 KB	C File
DSP_main.c	2 KB	C File
PhyEMIF.c	2 KB	C File
PhyFPGA.c	5 KB	C File
PhyGPIO.c	3 KB	C File
PhyInterrupts.c	3 KB	C File
PhyTimer1.c	4 KB	C File
Board.h	1 KB	H File
C6416RegisterDefs.h	9 KB	H File
Defs.h	3 KB	H File
DILUT.h	2 KB	H File
DlTimer1.h	1 KB	H File
DlVideoProcessing.h	1 KB	H File
PhyEMIF.h	1 KB	H File
PhyFPGA.h	1 KB	H File
PhyFPGARegisters.h	7 KB	H File
PhyGPIO.h	1 KB	H File
PhyInterrupts.h	1 KB	H File
PhyTimer1.h	1 KB	H File
DSP_Debug.cmd	2 KB	Windows NT Comm...

Figure 7.2 : DSP subdirectory. C source code, interrupt vector file and the memory command file.

B.3 Matlab/Simulink Models

Name	Size	Type
pulseEval.mdl	285 KB	Simulink Model
TxpTCC_VHDL_Test.mdl	907 KB	Simulink Model
TxP.mdl	185 KB	Simulink Model

Figure 7.3 : Simulink subdirectory. Simulink co-simulation and TxP implementation models.

B.4 High Resolution System Test Results Images



















Name ▲	Size	Type
 Figure 6.4.png	25 KB	PNG Image
 Figure 6.5.png	35 KB	PNG Image
 Figure 6.6.png	31 KB	PNG Image
 Figure 6.7.png	19 KB	PNG Image
 Figure 6.8.png	27 KB	PNG Image
 Figure 6.9.png	26 KB	PNG Image
 Figure 6.10.png	17 KB	PNG Image
 Figure 6.11.png	10 KB	PNG Image
 Figure 6.12.png	26 KB	PNG Image
 Figure 6.13.png	21 KB	PNG Image
 Figure 6.15.png	454 KB	PNG Image
 Figure 6.16.png	405 KB	PNG Image
 Figure 6.18.png	427 KB	PNG Image
 Figure 6.21.png	838 KB	PNG Image
 Figure 6.22.png	421 KB	PNG Image
 Figure 6.23.png	650 KB	PNG Image
 Figure 6.24.png	666 KB	PNG Image
 Figure 6.25.png	6 KB	PNG Image

Figure 7.4 : System test results images subdirectory.